Table of Contents

List of Tables

List of Figures

4.10 Shutdown Plant Problems

Learning Objectives:

1. List two major accident sequences identified at low power and shutdown plant conditions.

2. Describe the differences between full power and low power/shutdown major accident sequence classes.

3. List three systems and their components that have a history of becoming pressure locked.

4. Describe the alignment of the Residual Heat Removal System and Recirculation System when in shutdown cooling mode of RHR.

5. List the Technical Specifications violations from the events log.

4.10.1 Introduction

In 1989 the Nuclear Regulatory Commission initiated a program to examine the potential risks presented during low power and shutdown conditions. Two plants, Surry (PWR) and Grand Gulf (BWR), were selected to be studied. These studies (NUREG/CR-6143) along with operational experiences indicated that the risk during low power and shutdown conditions may be significant.

The risk associated with Grand Gulf operating in modes 4 and 5 was shown to be comparable with the risk associated with full power operation, 10^{-6} range. While the risk is low, very few systems/features of the plant are required to be available to attenuate a release should it occur. Technical specifications permits more equipment to be inoperable during low power and shutdown conditions. In certain plant conditions, primary containment is not required.

Figure 4.10-2 presents a comparison of the mean core damage frequency percentages for the major classes of accidents from both the full-power NUREG-1150 and the low power and shutdown mode analyses NUREG/CR-6143. From this figure, obvious similarities and differences can be seen. The major similarity observed is that in both analyses the station blackout (SBO) class is important. In the full power analysis SBOs are dominate accident sequences due to the loss or degradation of multiple systems. In operating mode 3 and 4 SBOs also show up because they still cause loss or degradation of multiple systems. However, there are additional accidents that can cause loss or degradation of multiple systems because of considerations unique to those modes of operation.

The major differences in the accident progression associated with the SBOs are:

- Almost all low power and shutdown mode SBOs sequences lead to an interfacing system LOCA where as the full power sequences do not.
- The containment is always open at the start of the low power and shutdown accidents whereas it is isolated at the start of the full power accidents.
- The probability of arresting core damage in the vessel is greater for full power accidents than for low power and shutdown conditions.

The remaining classes of accidents indicates a major differences between the two analyses. In the full power analysis, the anticipated transient without scram (ATWS) class is the second most important class while in the low power and shutdown analysis the second most important is SBO, with LOCA being number one. Given the plant conditions analyzed in the two studies, the first point that can be made is that ATWS sequences were simply not possible with the plant already in a shutdown state. On the other hand, since LOCAs were possible in both analyses, why did this class only show up in low power and shutdown results? While no detailed examination of this phenomenon was undertaken, the most likely reason for the appearance of LOCAs results is the intentional disabling of the automatic actuation of the suppression pool makeup system which is unique to the Mark III containment. Defeating automatic actuation of the suppression pool makeup is done for safety reasons. As a result, the continued use of injection systems during a LOCA require operator intervention. The difference in reliability between automatic actuation and operator action generally accounts for the fact that LOCAs survived in the low power and shutdown analysis but not in the full power analysis.

4.10.2 Binding of Gate Valves

Thermal binding of double-disc and flexible-wedge gate valves has been addressed by the NRC and the industry since 1977. Particularly, throughout the 1980's the industry issued a number of event reports concerning safety-related gate valve failures due to disc-binding. These failures were attributed to either pressure locking or thermal binding. Binding of gate valves in the closed position is of safety concern because gate valves have a variety of applications in safety-related systems and may be required to open during or immediately following a postulated event. During such events, valve performance is severely challenged by the rapid cooldown and depressurization rates which expose the disc to large differential pressures.

Generally valve operators are not sized to open a valve against binding forces. Pressure locking or thermal binding of gate valves represents a nonrevealing common-mode failure mechanism since normal surveillance tests may not detect or identify them.

Safety-related systems for a BWR in which valves have become pressure locked include:

- HPCI - Steam admission valve
- LPCS - Injection valve
- LPCI - Injection valve
- RCIC - Steam admission valve
- RR - Recirc pump discharge valve

A review of the events shows that there were two potential causes of pressure locking; liquid entrapment in the bonnet and high ΔP across the disc while in the closed position. Most of the events occurred during infrequent plant evolutions such as heat-up, cooldown, and testing. Pressure locking adversely affects operation of motor operated valves, and renders the associated system unavailable.

4.10.2.1 Thermal Binding Phenomenon

If a wedge gate valve is closed while the system is hot, thermal binding can occur as the system cools. The valve body and discs mechanically interfere because of their different thermal expansion and contraction characteristics. The difference in thermal contraction can cause the seats to bind the disc so tightly that reopening is extremely difficult or impossible until the valve is reheated. Several potential remedies have been suggested to alleviate this situation:

- Slightly opening and reclosing a valve periodically during a cooldown.
- Limiting valve actuator closing forces.
- Using compensating spring packs to reduce valve initial closing forces.

In general, neither ac nor dc valve motor operator sizing analyses account for the extra force needed to unseat a valve when it is thermally bound.

4.10.2.2 Pressure Locking Phenomenon

Pressure locking in flexible-wedge and double-disc gate valves generally develops because of valve design in combination with characteristics of the bonnet and specific local conditions at the valve (temperatures and pressures). The essential feature to develop pressure locking is the presence of fluid in the bonnet cavity, including the area between the discs. The fluid may enter the bonnet cavity during normal opening and closing valve cycle. Also, fluid may enter the bonnet cavity of a closed valve which has a ΔP across the disc. The pressure differential causes the disc to move slightly away from the seat , developing a flow path for fluid so that the bonnet cavity becomes filled with high pressure fluid. Whether these situations lead to a valve pressure locking scenario depends upon the pressure of the fluid that enters the bonnet cavity, and the difference in pressure between the process fluid and bonnet cavity at the time the MOV is called upon to operate.

4.10.2.3 Consequences of Locking

These phenomena can delay the valve stroke time or cause the valve motor actuator to stall. Events at Susquehanna and FitzPatrick indicate that the RHR/LPCI and LPCS injection valves of a BWR are susceptible to pressure locking caused by bonnet cavity pressurization. In both systems the injection valve is normally shut and is require to automatically open upon receipt of an actuation signal. The testable check valve located between the reactor and injection valve is not a leak-tight valve. Leakage past the check valve can pressurize the piping between the valves and the injection valve cavity to reactor pressure. Near leak-tight seating surfaces of the injection valve may allow the valve cavity to remain pressurized and become subject to pressure locking when injection is needed during a LOCA. Under this condition, the bonnet pressure is greater than 1000 psig, while the downstream pipe suddenly depressurizes to between 400 and 500 psig. This high internal-to-externa lΔP across both seating surfaces would result in double-disc drag forces, which if they exceed the available thrust of the actuator, will produce pressure locking.

When a valve disc becomes locked in the closed position due to pressure locking or thermal binding, actuation of the motor will result in locked-rotor current which will rapidly increase the temperature of the motor internals. Within 10 to 15 seconds, the heat buildup can degrade the motor's capability to deliver a specified torque, damage the motor, or both.

4.10.3 Mode 3/4 Event

Hope Creek is a BWR/4 plant rated at 3293 MWt and 1067 MWe with a Mark I containment. At the time of the event the plant was operating in an action statement requiring the plant to shutdown in seven days due to an inoperable control room ventilation component. The allowed operating time of seven days was approaching expiration so the plant had commenced a reactor shutdown. As part of the normal shutdown procedure the reactor was manually scrammed by placing the mode switch in the shutdown position. The plant entered operating mode 3 at 12:18 am on July 8, 1995. Table 4.10-1 lists the sequence of events and provides a detailed description of the event to conclusion.

By using the sequence of events, attached figures, technical specifications and this text, answer learning objectives 4 and 5 in this chapter.

4.10.4 Summary

The reader should be aware that the statistics presented herein are for Grand Gulf. As such, this information should not be generalized to other nuclear power plants without first considering all relevant factors. Complete details of the Grand Gulf statistics and insights can be found in SAND94-2949.

What can be generalized, is the apparent change in dominant accident sequences from full power to low power and shutdown conditions. This is extremely important when you consider that technical specifications action statements usually require you to go to mode 3 or 4 within some time frame. The NRC felt so concerened about the apparent change in risk when entering modes 3 and 4 that they enlisted Sandia National Laboratories to evaluate the risk impact of the Limiting Conditions of Operation (LCOs) in the current Grand Gulf technical specifications. The results of the study were published in NUREG/CR-6166.

Table 4.10-1 Sequence of Events

July 8, 7:00 am	Operating Shift turnover
7:54	The B RHR pump was placed in service to establish shutdown cooling (SDC) in accordance with procedures. Indicated RHR flow was approximately 10,000 gpm.
7:54 to 9:40	The A and B recirculation pump discharge valves were stroked open and closed to prevent thermal binding in the closed position.
9:40	Nuclear controls operator unsuccessfully attempted to open the 'A' recirculation pump discharge valve.
9:50	Nuclear controls operator unsuccessfully attempted to open the 'A' recirculation pump discharge valve a second time. An action request was initiated to investigate and correct the valve failure.
10:57	Operating mode 4 is reached
11:00	The nuclear controls operator partially opened and left open the 'B' recirculation pump discharge valve to prevent thermal binding in the closed position.
11:52	Reactor pressure indicated zero pounds per square inch gage (psig) and the reactor vessel head vent valves to the equipment drain sump were opened in accordance with procedures.
12:59 pm	The electrical supply breaker for the reactor water cleanup supply line inside isolation valve (F001) was opened to support a corrective maintenance activity.
2:38	All high reactor pressure automatic isolation signals for the inboard and outboard shutdown cooling isolation valves were defeated. In addition, the isolation capabilty was defeated for the inboard valve. These signals were defeated in accordance with procedures, to prevent an inadvertent isolation and also in preparation for reactor protection system surveillance testing.
4:35	The shutdown cooling system was secured to facilitate manual operation of the RHR shutdown cooling isolation valves, per procedure, to verify that the valves could be closed manually. This is a precautionary step performed following defeat of the automatic signals.
5:09	Shutdown cooling was returned to service. The RHR heat exchanger inlet temperature promptly increased from 163 degrees to 182 degrees fahrenheit.
5:30	Operators entered the drywell to perform outage activities, assess a drywell cooler leak and to investigate the reason for recirculation pump discharge valve failure.
5:54	Electrical supply breaker for the reactor water cleanup valves was reclosed.
6:45	Operators manually "cracked" open the 'A' recirculation pump discharge valve. Upon exiting the drywell, plant operators reported condensation on drywell surfaces and also fogging of their glasses. The nuclear controls operator opened 'A' recirculation pump discharge valve until he received an electrical dual indication.
7:00	Operating shift turnover

Table 4.10-1 Sequence of Events (Continued)

8:00 pm	The senior nuclear shift supervisor (SNSS) turnover completed, however, the on coming SNSS was involved with other activities and missed the shift briefing.
8:30	SNSS and NSS performed a control room panel walkdown and noted the 2000 gpm of recirculation system flow. They decided to shut the recirculation pump discharge valves.
8:45	The drywell primary containment instrument gas system was tagged out and depressurized in preparation for outage maintenance activities.
9:00	The nuclear controls operator closed the 'A' recirculation pump discharge valve after RHR heat exchanger inlet temperature decreased to 155 °F and the thermal binding limitation was no longer applicable. An attempt was made to also close the discharge valve for the 'B' pump, but was unsuccessful. The nuclear controls operator assumed this was due to some valve control interlock and decided to open the valve further and try again to close it.
10:00 to 11:00	The nuclear controls operator noted reactor pressure was indicating approximately 17 psig, but was not confident about the accuracy of the pressure indication at the low end of a 0 - 1500 psig meter. The electrical supply breaker for the RWCU F001 valve was opened in preparation for transferring the RPS system to its alternate power supply.
11:00	The operators noted that drywell floor drain leakage had increased to 1-2 gpm.
July 9, 00:30	RWCU valve F001 was returned to an operable status.
1:00 am	The nuclear controls operator noted that a shutdown cooling high pressure trip unit indicated 60 psig. The operator directed an instrument technician to accurately determine reactor pressure. The reading taken indicated pressure between 19 and 24 psig on all channels.
1:30	The operating crew decided to enter the drywell and identify the source of drywell leakage and to manually shut 'B' recirculation pump discharge valve.
4:29	The automatic isolation signals for shutdown cooling inboard and outboard suction valves were restored to normal.
4:49	The automatic isolation signals for shutdown cooling inboard and outboard isolation valves were again bypassed.
4:54	Shutdown cooling was secured and attempt was made to close 'B' recirculation pump discharge valve. In the attempt, the valve was fully opened.
5:00	SNSS and NSS discussed closing the 'B' recirculation pump suction valve as a contingency plan.
5:08	Shutdown cooling was restored. RHR heat exchanger inlet temperature increased approximately 7 °F.
5:50	'B' recirculation pump discharge valve was closed manually, RHR inlet temperature increased to 191 °F along with vessel bottom head temperature from 150 to 189 °F, in about 2 minutes. Reactor pressure started trending down toward zero.

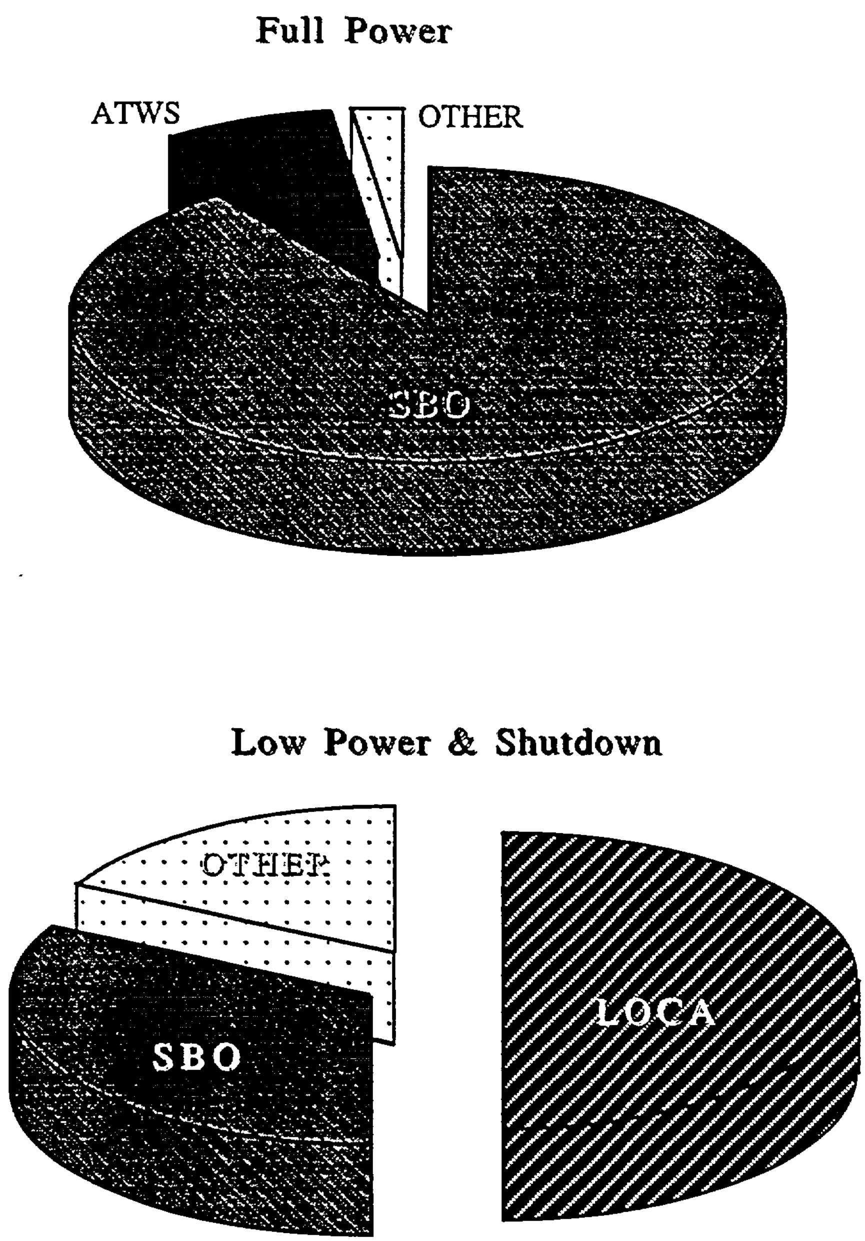


Figure 4.10-1 Accident Sequence Comparison

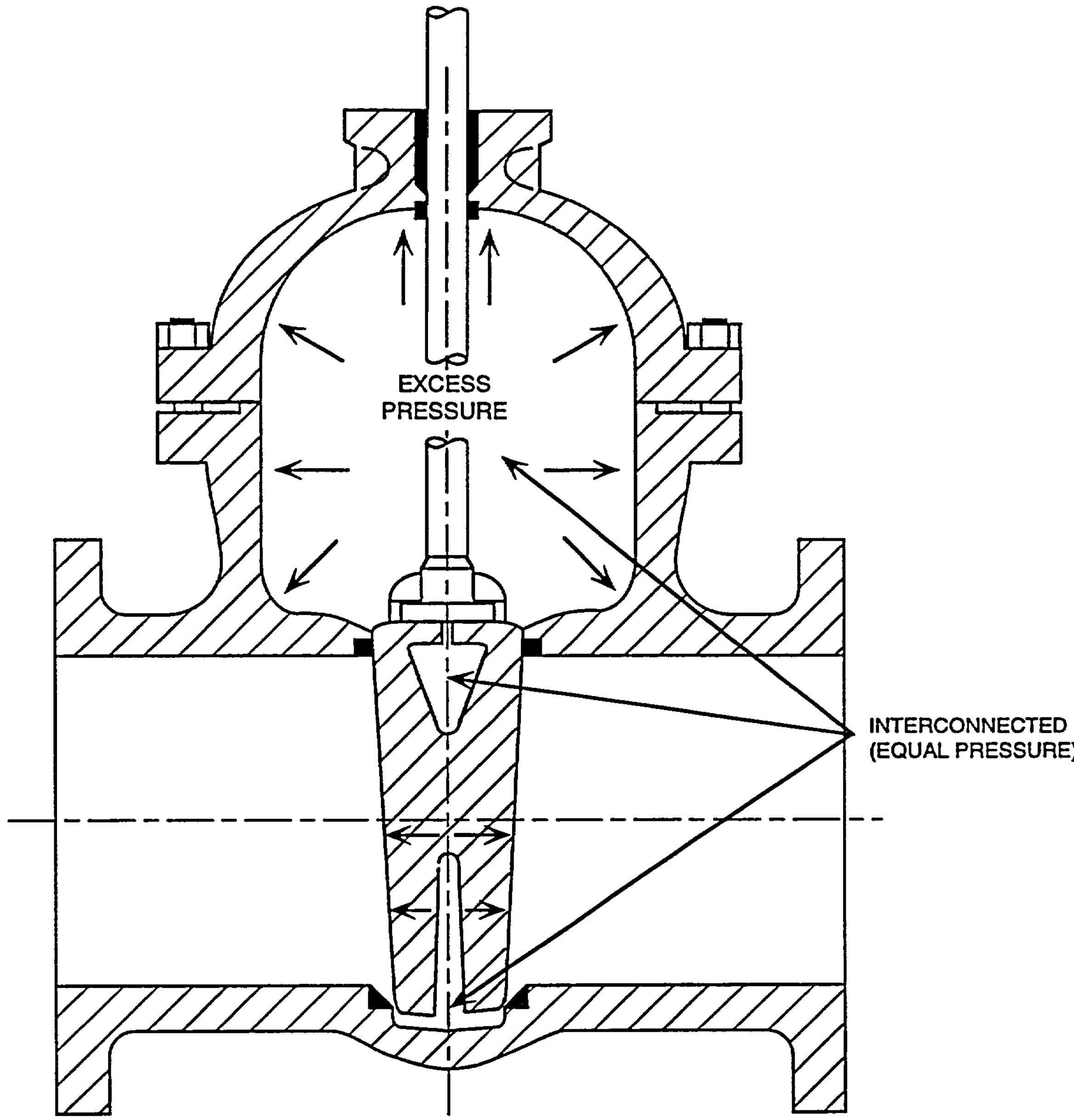


Figure 4.10-2 Pressure Locking Flexible-Wedge Gate Valve

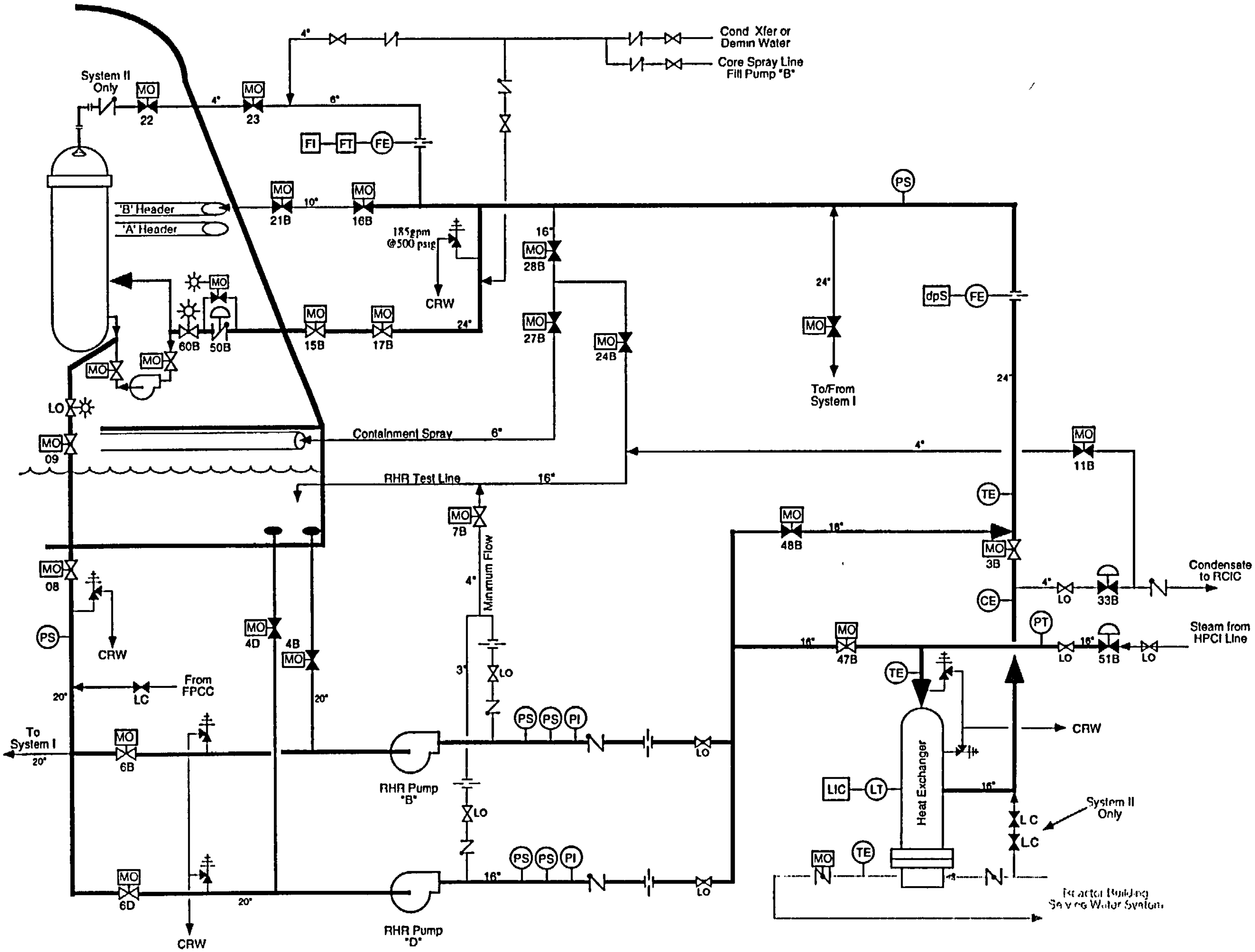


Figure 4.10-3 RHR System Shutdown Cooling Mode

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ATTACHMENTS

4.11 RISK MANAGEMENT

Learning Objectives:

1. Describe what is meant by the term "defense in depth," and explain how nuclear power plants have been designed to incorporate this concept.

2. Describe how probabilistic risk assessments (PRAs) of nuclear power plants can complement deterministic analyses.

3. Define the term "configuration management," and explain why configuration management is necessary in managing risk at nuclear power plants.

4. Describe methods that are used by nuclear utilities to incorporate risk insights into maintenance planning.

5. Describe how PRA results are used by the NRC for risk- informed regulation.

4.11.1 Introduction

Nuclear power plants in the U.S. have been designed and constructed in accordance with deterministic analyses. The design bases of each nuclear unit are documented in its Final Safety Analysis Report (FSAR), which is updated yearly as the Updated Safety Analysis Report (USAR). Nuclear power plant operation, including maintenance and surveillance of safety-related equipment, is controlled and restricted by technical specification requirements.

Throughout the history of commercial nuclear power, the regulatory agencies (the AEC and later, the NRC) and the nuclear industry have continued to research and implement new and/or better methods of operating, maintaining, testing, and analyzing nuclear plants and equipment to reduce risk and to ensure safety. This section discusses the major regulatory and industry actions that have been or are being incorporated to address operational and accident risk management in nuclear power plants.

4.11.2 History

4.11.2.1 Deterministic Analysis

Nuclear power plants in the U. S. have been designed and constructed in accordance with deterministic analyses. Deterministic analyses involve standard good engineering practices, calculations, and judgements; and in the case of nuclear power plants, design bases which include the assumption of worst-case conditions for accident analyses. Examples of these worst-case conditions include the assumptions of an initial reactor power of greater than 100%, restrictive power distributions within the core, conservative engineering factors, the minimum-required accident mitigation equipment available, and pipe breaks of all possible sizes.

In a large nuclear generating station with a core output rated at over 3000 MW thermal, about six pounds of fission products are produced each day that the unit is operated at full power. To protect the public from these fission products during normal and accident situations, a "defense in depth," or multiple levels of assurance and safety, exists to minimize risk to the public from nuclear power plant operation.

A multiple barrier concept was used in designing and building nuclear units. The first barrier against fission product release is the fuel cladding. The fuel cladding consists of an enclosed cylindrical cylinder that is designed to contain fuel pellets and fission products during normal and abnormal transients. The second barrier, if isolated, is the reactor coolant pressure boundary. The containment systems, primary and secondary containment, provide two additional distinct fission product barriers. These barriers and the protection against the loss of each barrier are required by the Code of Federal Regulations.

Engineered safety features (ESFs) are provided in nuclear power plants to mitigate the consequences of reactor plant accidents. Sections of the General Design Criteria in Appendix A of 10 CFR, Part 50 require that specific systems be provided to serve as ESF systems. Containment systems, a residual heat removal (RHR) system, emergency core cooling systems (ECCSs), containment heat removal systems, containment atmosphere cleanup systems, and certain cooling water systems are typical of the systems required to be provided as ESF systems. Each of the ESF systems is designed to withstand a single failure without the loss of its protective functions during or following an accident condition. However, this single failure is limited to either an active failure during the injection phase following an accident, or an active or a passive failure during the recirculation phase. Most accident analyzes assume the loss of offsite power. This loss of offsite power is considered in addition to the "single active failure."

The engineered safety features which contain active components are designed with two independent trains. Examples of systems employing this design feature are the ECCSs, in which either train can satisfy all the requirements to safely shut down the plant or meet the final acceptance criteria following an accident. Redundant pumps, valves, instrument sensors, instrument strings, and logic devices are required to ensure that no single failure will prevent at least one of these trains from performing its intended function.

All engineered safety feature systems must be physically separated so that a catastrophic failure of one system will not prevent another engineered safety feature system from performing its intended function. Electrical power to the engineered safety features comes from the transmission grid via transformers, breakers and busses. Redundant diesel generators are normally the standby power supply.

ESF systems are designed to remain functional if a safe shutdown earthquake occurs and are thus designated as Seismic Category I. The reactor coolant pressure boundary, reactor core and vessel internals, and systems or portions of systems that are required for emergency core cooling, post-accident containment heat removal, and post-accident containment atmosphere cleanup are designed to Seismic Category I requirements. ESF systems are also designed to include diversity. "Diversity" refers to different methods of providing the same safety protection or function. Two systems which illustrate diversity are the core spray system and residual heat removal system; both are low pressure ECCSs. Both of these systems are designed to mitigate the consequences of a loss of coolant accident (LOCA). However, the core spray system provides core cooling by spray and flooding, while the residual heat removal system utilizes flooding alone.

4.11.2.2 Probabilistic Risk Assessment

A PRA is an engineering tool used to quantify the risk to a facility. Risk is defined as the likelihood and consequences of rare events at nuclear power plants. These events are generally referred to as severe accidents. The PRA augments traditional deterministic engineering analyses by providing quantitative measures of safety and thus a means of addressing the relative significance of issues in relation to plant safety. Basically, a nuclear power plant PRA answers three questions:

- What can go wrong?
- How likely is it?
- What are the consequences?

Probabilistic risk assessment is a multidisciplinary approach employing various methods, including system reliability, containment response modeling, and fission release and public consequence analyses, as depicted graphically in Figure 4.11-3. A PRA treats the entire plant and its constituent systems in an integrated fashion, and thus subtle interrelationships can be discovered that are important to risk. Another important attribute of probabilistic risk assessment is that it involves analyses of both single and multiple failures. Multiple failures often lead to situations beyond the plant design basis and, in some cases, are more likely than single failures. By addressing multiple failures, a PRA can cover a broad spectrum of potential accidents at a plant.

The first comprehensive development and application of PRA techniques in the commercial nuclear power industry was the NRC-sponsored "Reactor Safety Study" (RSS). The principal objective of the RSS was to quantify the risk to the public from U.S. commercial nuclear power plants. The RSS analyzed both a BWR (Peach Bottom) and a PWR (Surry). The report of the RSS results, generally referred to as WASH-1400, was published in October of 1975. The results of the study can be summarized as follows: (1) risks from nuclear power plant operation are small as compared to non-nuclear hazards; (2) the frequencies of core melt accidents are higher than previously thought (calculated to be approximately 5×10^{-5} per reactor year); (3) a variety of accident types are important; (4) design-basis accidents are not dominant contributors to risk; and (5) significant differences in containment designs are important to risk. The basic PRA approach developed by the RSS is still used today.

Because the RSS was the first broad-scale application of event- and fault-tree methods to a system as complex as a nuclear power plant, it was one of the more controversial documents in the history of reactor safety. The RSS also analyzed conditions beyond the design basis and attempted to quantify risk. A group called the Lewis Committee performed a peer review of the RSS and published a report, NUREG/CR-0400, to the NRC three years later to describe the effects of the RSS results on the regulatory process. The report concluded that although the RSS had some flaws and that PRA had not been formally used in the licensing process, PRA methods were the best available and should be used to assist in the allocation of the limited resources available for the improvement of safety.

The 1979 accident at Three Mile Island (TMI) substantially changed the character of the NRC's regulatory approach. The accident revealed that perhaps nuclear reactors might not be safe enough and that new policies and approaches were required. Based on comments and recommendations from the Kemeny and Rogovin investigations of the TMI accident, a substantial program to research severe accident phenomenology was initiated (i.e., those accidents beyond the design basis which could result in core damage). It was also recommended that PRA be used more by the staff to complement its traditional, non-probabilistic methods of analyzing nuclear plant safety. Rogovin also suggested in a report to the Commissioners and the public, NUREG/CR-1250, that the NRC policy on severe accidents consider (1) more severe accidents in the licensing process and (2) probabilistic safety goals to help define what is an acceptable level of plant safety.

In late 1980, the NRC sponsored a current assessment of severe accident risks for five commercial nuclear power plants in a report called "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," NUREG-1150. This report included an update of the RSS risk assessments of Surry and Peach Bottom and provided the latest NRC version of the state of the art in PRA models, methods, and approaches.

A summary of the insights gained from early risk assessments are as follows:

1. As illustrated by the NUREG-1150 results and early plant PRAs, the PRAs reflect details of plant systems, operations and physical layouts. Since nuclear power plants in the U.S. are not standardized, the PRA results are very plant specific. Reactor design, equipment, location, and operation (power levels, testing and maintenance, operator actions) have large impacts on the results. Therefore, in detail, the results can differ significantly from plant to plant.

2. Even with the differences in the detailed results between plant studies, PRAs can be used for some generic applications as listed in NUREG-1050. Some examples are:

   - Regulatory activity prioritization,
   - Safety issue evaluation,
   - Resource allocation,
   - Inspection program implementation, and
   - NRC policy development.

3. Using PRA in the decision making process has aided licensees in determining which design modifications are desirable from both risk-reduction and cost-benefit standpoints for the improvement of plant safety. PRA results have more recently been used by licensees in enforcement discussions and in support of technical specification change requests.

4. PRAs have pointed out some general differences with respect to BWRs and PWRs as classes of plants. For example, NUREG-1150 states that for BWRs, the principal initiating event contributors to core damage frequency are station blackouts (SBOs) and anticipated transients without scram (ATWSs); for PWRs, the principal contributors to core damage frequency are LOCAs. NUREG-1150 also states that the core damage frequencies for PWRs are higher than those for BWRs, because BWRs have more redundant methods of supplying water to the reactor coolant system. However, PWRs have lower probabilities of early containment failure given a core-damage sequence, since PWR containments are larger and can withstand higher pressures than BWR containments.

4.11.2.3 Severe Accident Policy

In August of 1985, the NRC issued the "Policy Statement on Severe Accidents Regarding Future Designs and Existing Plants" that introduced the Commission's plan to address severe accident issues for existing commercial nuclear power plants. The stated policy was that the public should be subject to no undue risk from the operation of commercial nuclear reactors. A year later, in August of 1986, the NRC established both qualitative and quantitative safety goals for the nuclear industry. The qualitative safety goals are as follows:

- Individual members of the public should be provided a level of protection from the consequences of nuclear power plant operation such that individuals bear no significant additional risk to life and health.

- Societal risks to life and health from nuclear power plant operation should be comparable to or less than the risks of generating electricity by viable competing technologies and should not be significant additions to other societal risks.

The corresponding quantitative safety goals are:

- The risk to the average individual in the vicinity of a nuclear power plant of prompt fatalities that might result from a reactor accident should not exceed one-tenth of one percent of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. population are generally exposed.

- The risk to the population near a nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed one-tenth of one percent of the sum of cancer fatality risks resulting from all other causes.

The average accident fatality rate in the U.S. is approximately 5×10^{-4} per individual per year, so the quantitative value for the first goal is 5×10^{-7} per individual per year. The "vicinity of a nuclear power plant" is defined to be the area within one mile of the plant site boundary. The average U.S. cancer fatality rate is approximately 2×10^{-3} per year, so the quantitative value for the second goal is 2×10^{-6} per average individual per year. The "population near a nuclear power plant" is defined as the population within 10 miles of the plant site.

However, because of arbitrary assumptions in calculations, uncertainties in PRA analyses, and gaps in equipment reliability data bases, the safety goals are not definitive requirements, but serve as aiming points or numerical benchmarks. In addition, it should be noted that the goals apply to the industry as a whole and not to individual plants. The safety goals are not in and of themselves meant to serve as the sole bases for licensing decisions. However, when information is available that is applicable to a specific licensing decision, it is to be considered as one factor in the licensing.

Implementation of the NRC plan to address severe accident risk included development of plant-specific examinations that would reveal vulnerabilities to severe accidents and cost-effective safety improvements that would reduce or eliminate the important vulnerabilities. In Generic Letter 88-20 dated November 23, 1988, all utilities with licensed nuclear power plants were requested to perform such examinations. The specific objectives for these individual plant examinations (IPEs) are for each utility to:

- Develop an overall appreciation of severe accident behavior,

- Understand the most likely severe accident sequences that could occur at its plant,

- Gain a more quantitative understanding of the overall probability of core damage and radioactive material releases, and

- If necessary, reduce the overall probability of core damage and radioactive material release by appropriate modifications to procedures and hardware that would help prevent or mitigate severe accidents.

Many of the IPEs submitted to the NRC have identified unique and/or important safety features. Table 4.11-1 includes a list of insights obtained through analysis of 72 IPEs (25 BWRs and 47 PWRs) covering 106 commercial nuclear units (35 BWRs and 71 PWRs). The items in the list indicate vulnerabilities identified during the IPE process at various plants and modifications that may have been made to plant equipment or procedures to reduce the vulnerabilities and hence, the calculated core damage frequencies.

Risk- and reliability-based methods can be used for evaluating allowed outage times, scheduled or preventive maintenance, action statements requiring shutdown where shutdown risk may be substantial, surveillance test intervals, and analyses of plant configurations resulting from outages of systems or components. Because of the limitations in the IPE process such as arbitrary assumptions in calculations, uncertainties in PRA analyses, and gaps in equipment reliability data bases, the insights identified in and of themselves do not require any action by the individual licensee, but provide information on where vulnerabilities exist in its plant.

4.11.3 Risk-Based Regulation

Technical specification requirements for nuclear power plants define the limiting conditions for operation (LCOs) and surveillance requirements (SRs) to assure safety during operation. In general, these requirements are based on deterministic analyses and engineering judgements. Experiences with all modes of plant operation indicate that some elements of the requirements are unnecessarily restrictive, while a few may not be conducive to safety. Improving these requirements involves many considerations and is facilitated by the availability of plant-specific IPEs and the development of related methods for analysis. Risk-based regulation is a regulatory approach in which insights from PRAs are used in combination with deterministic system and engineering analyses to focus licensee and regulatory attention on issues commensurate with their importance to safety.

Examples of uses of risk insights for risk-based regulation include the prioritization of generic safety issues, evaluation of regulatory requirements, assessment of design or operational adequacy, evaluation of improved safety features, prioritizing inspection activities, evaluation of events, and evaluation of technical specification revision requests and enforcement issues.

Using risk- and reliability-based methods to improve technical specifications and other regulatory requirements has gained wide interest because they can:

- Quantitatively evaluate risk impacts and justify changes in requirements based on objective risk arguments, and

- Provide a defensible bases for improved requirements for regulatory applications.

Caution must be applied when using the results of risk assessments, however, because of the limitations of PRA methodology. The plant's initial PRA (and/or IPE) is a snapshot of the plant at the time the plant configuration and data were collected and analyzed. The analyses must be revised as modifications are made to the plant design, operating methods, procedures, etc., to maintain the risk assessment results current. In addition, a PRA model is not a complete or accurate model of the plant during all modes of operation. For example, for PWRs, the removal of both boric acid makeup pumps from service is not very risky during mode 1 operations; however, these pumps are very important when the achievement of the required shutdown margin in mode 5 is considered. Other limitations of PRAs include the uncertainties in the equipment failure data bases, the level of understanding of physical processes, the uncertainties in quantifying human reliability, the sensitivity of results to analytical assumptions, and modeling constraints.

Quantitative risk estimates have played an important role in addressing and resolving regulatory issues including:

- Anticipated transient without scram: Risk assessments contributed to development of the ATWS rule, 10CFR50.62, which requires all PWRs to have equipment diverse and independent from the reactor protection system for auxiliary feedwater initiation and turbine trip, requires all CE and B&W PWRs and BWRs to have a diverse scram system, provides functional requirements for the standby liquid control systems of BWRs, and requires that BWRs have equipment for automatically tripping reactor coolant recirculation pumps.

- Auxiliary feedwater (AFW) system reliability: The NRC has reviewed information provided on auxiliary feedwater systems in safety analysis reports. As part of each review, the NRC assures that an AFW system reliability analysis has been performed. The Standard Review Plan states that an acceptable AFW system should have an unreliability in the range of 10^{-4} to 10^{-5}. Compensating factors such as other methods of accomplishing the safety functions of the AFW system or other reliable methods for cooling the reactor core during abnormal conditions may be considered to justify a larger unavailability of an AFW system.

- Station blackout (loss of all ac power): Risk assessments contributed to development of the blackout rule, 10CFR50.63, which requires licensees to determine a plant-specific station blackout duration, during which core cooling and containment intergrity would be maintained, and to have procedures addressing station blackout events. The rule allows utilities several design alternatives to ensure that an operating plant can safely shut down in the event that all ac power is lost. One alternative is the installation of a full-capacity alternate ac power source that is capable of powering at least one complete set of normal safe shutdown loads.

- Backfits: There are many cases where PRAs have been used to support the backfit decision process. For example, after the TMI accident several TMI action plan issues evolved. Consumers Power performed a PRA of the Big Rock Point nuclear plant to assist in identifying those TMI generated changes which might actually have an impact on the risk at the plant. As a result, Consumers Power was able to negotiate exemptions on seven issues which did not significantly lower risk at Big Rock Point, saving over $45 million. In addition, Consumers Power used the PRA to identify changes necessary to reduce the core damage frequency at Big Rock Point to an acceptable level. The cost of a change is generally considered to be the dollar cost associated with design, licensing, implementation, operation and maintenance. Sometimes the cost of replacement power is included for a backfit requiring a plant shutdown to implement. The benefit of the change is the reduction in risk if the change is implemented. The most cost-effective change provides the most improvement in safety for the least cost. This type of cost-benefit analysis was done extensively during the ATWS rule-making process.

- Risk-based inspections: A PRA provides information on dominant accident sequences and their minimal cut sets. This information has already been used to design the risk-based portions of some plant-specific inspection programs. Inspection programs can be prioritized to address the minimization of hardware challenges, the assurance of hardware availability, and the effectiveness of plant staff actions as they relate to the systems and faults included in the dominant accident sequences. A PRA supports the assessment of a plant change by providing a quantitative measure of the relative level of safety associated with the change. This is accomplished by performing sensitivity studies. A sensitivity study is a study of how different assumptions, configurations, data or other potential changes in the basis of the PRA impact the results.

The NRC staff is expected to use PRA results to assist in prioritizing regulatory activities, and plant inspectors are expected to use IPE results to prioritize inspection activities. The inspectors should be alert for situations which constitute near misses. That is, the inspector needs to recognize those events that come close to accident sequences. Recognizing the significance of events at the plant is especially important for those related to sequences initiated by an ATWS or an intersystem LOCA, which can have severe consequences. Finally, the NRC staff will be involved in more and more discussions in which PRA results are used or misused to justify a particular action or inaction. Therefore, it is important that the staff be familiar with the types of information that a PRA provides and that the staff can use PRA information accurately in discussions and decisions.

4.11.4 PRA Policy Statement and Implementation Plan

Deterministic approaches to regulation consider a set of challenges to safety and determine how those challenges should be mitigated. A probabilistic approach to regulation enhances and extends the traditional deterministic approach by:

- Allowing consideration of a broader set of potential challenges to safety,
- Providing a logical means for prioritizing these challenges based on risk significance, and
- Allowing consideration of a broader set of resources to defend against these challenges.

In August of 1995, the NRC issued the "Policy Statement on the Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities." The overall objectives of the policy statement are to improve the regulatory process through improved risk-informed safety decision making, through more efficient use of staff resources, through a reduction in unnecessary burdens on licensees, and through the strengthening of regulatory requirements. The policy statement contains the following elements regarding the expanded NRC use of PRA:

- Increased use of PRA in reactor regulatory matters should be implemented to the extent supported by the state of the art in PRA methods and data and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy.

- PRA should be used to reduce unnecessary conservatism associated with current regulatory requirements. Where appropriate, PRA should be used to support additional regulatory requirements.

- PRA evaluations in support of regulatory decisions should be as realistic as possible, and appropriate supporting data should be publicly available.

- Uncertainties in PRA evaluations need to be considered in applying the Commission's safety goals for nuclear power plants.

An agency-wide plan has been developed to implement the PRA policy statement. The scope of the PRA implementation plan includes reactor regulation, reactor safety research, analysis and evaluation of operational experience, staff training, nuclear material, and low and high level waste regulations. The plan provides mechanisms for monitoring programs and management oversight of PRA-related activities. The plan includes both ongoing and new PRA-related activities. The following are PRA-related regulatory activities that are underway within the NRC:

- Graded quality assurance,
- The maintenance rule,
- In-service inspection and testing,
- The IPE insights program,
- PRA training for the staff, and
- The reliability data rule.

4.11.4.1 Risk Management

Risk management is a means of prioritizing resources and concerns to control the level of safety. As discussed above, the NRC's and nuclear industry's use of risk analyses have shown that:

- The risk from nuclear power plant operation is generally low,
- Low cost improvements can sometimes have significant safety and economic benefits, and
- Subtle design and operational differences make it difficult to generalize dominant risk contributors from plant to plant or for a class of plants.

Because each nuclear power plant is essentially unique, the most powerful use of the PRA is as a plant-specific tool. PRAs can be used in two basic ways:

1. To support plant operations, maintenance, inspection, and planning activities; and
2. To provide information regarding changes to improve plant safety and reliability.

A plant's PRA can be used during all modes of plant operation to prioritize operations and maintenance resources to maintain safety at acceptable levels. This is accomplished, in part, by periodically updating the PRA results to keep current with plant configuration and component failure data. Importance measures can be used to indicate where preventive actions would be most beneficial and what is most important to maintain at acceptable safety levels. Based on the updated results, adjustments in plant activities and design can be made, as appropriate, to maintain the desired level of safety as indicated by the results of the PRA.

The PRA supports plant activities by providing information on the risk-significant areas in plant operation, maintenance, and design. Operations, maintenance, inspection, and planning personnel can then appropriately address these areas to control the risk at acceptable levels.

The risk-significant areas are identified by the results of the PRA. These areas are where the most attention and effort should be focused. Several useful PRA results are (1) dominant contributors (these indicate which failures are the largest contributors to the likelihood of accident sequences), (2) dominant accident sequences (these depict the failure paths that contribute most to core damage frequency), and (3) importance measures (these evaluate what contributes most to core damage, what would reduce the core damage frequency the most, and what has the greatest potential for increasing core damage frequency should it not be as reliable as desired). The major contributors to core damage by accident type for the NUREG-1150 PWR and BWR plants are shown in Figure 4.11-5, and the relative importance of BWR and PWR systems from NUREG-1050 are shown in Figures 4.11-6 and 4.11-7.

PRA results can be used in many ways during planning and operational activities at a nuclear plant. The results have an important role in risk management, maintenance planning, and risk-based inspections.

4.11.4.2 Configuration Management

Configuration management is one element of risk management and risk-based regulation. Configuration risk refers to the risk associated with a specific configuration of the plant. A configuration usually refers to the status of a plant in which multiple components are simultaneously unavailable. The risk associated with simultaneous outages of multiple components can be much larger than that associated with single-component outages. Technical specifications forbid outages of redundant trains within a safety system, but many other combinations of component outages can pose significant risk. In controlling operational risk, these configurations need to be analyzed. The configuration management process can be predictive in planning maintenance activities and outage schedules, and can be retrospective in evaluating the risk significance of plant events.

When a component is taken out of service for maintenance or surveillance, it has an associated downtime and risk. If the component is controlled by an allowed outage time in the Technical specifications, then this downtime is limited by the allowed outage time. Configuration management involves taking measures to avoid risk-significant configurations. It involves managing multiple equipment taken out of service at the same time, the outage times of components and systems, the availability of backup components and systems, and outage frequencies.

4.11.4.3 On-Line Maintenance

Licensees are increasing the amount and frequency of maintenance performed during power operation. Licensees' expansion of the on-line maintenance concept without thorough consideration of the safety (risk) aspects raises significant concerns. The on-line maintenance concept extends the use of technical specification allowed outage times beyond the random single failure in a system and a judgement of a reasonable time to effect repairs upon which the allowed outage times were based. Compliance with GDC single failure criteria is demonstrated during plant licensing by assuming a worst-case single failure, which often results in multiple equipment failures. This does not imply that it is acceptable to voluntarily remove equipment from service to perform on-line maintenance on the assumption that such actions are bounded by a worst-case single failure.

A simplified qualitative model (shown graphically in Figure 4.11-12) for evaluating risk can be thought of as including three factors combined in the following way:

$$\text{Risk} = P_i \times P_m \times P_c$$

Where:

P_i = The probability of an initiating event, such as a LOCA, turbine trip, or loss of offsite power.

P_m = The probability of not being able to mitigate the event, with core damage prevention as the measure of successful mitigation.

P_c = The probability of not being able to mitigate the consequences, with containment integrity preservation as the measure of success.

The intersection of all three occurrences (initiating event occurs + mitigating equipment fails + containment fails) indicates a worst-case scenario, with core melt and subsequent radioactive release to the public (a Chernobyl-type event, for example). The intersection of the initiating event and mitigating equipment failure would be a TMI-type event, in which there is core melt without a release. If the consequence of an event is defined as financial loss (a viable definition), one would have to say that this intersection represents a serious scenario itself. Even considering the traditional definition of consequence (potential for core melt), the intersection of an initiating event and mitigating equipment failure is of concern to the utility and to the NRC.

An effective risk-assessment process includes consideration of the impact of maintenance activities on all three of these risk factors. It also considers the impact of maintenance activities on both safety-related and non-safety-related equipment. Multiple or single maintenance activities that simultaneously, or within a short time frame, impact two or more risk factors tend to increase risk the greatest. In addition, on-line maintenance tends to increase component unavailabilities. With increased scheduling of maintenance during power operation, the overall impact on train unavailability, when averaged over a year, has in many cases increased dramatically and in some cases to the point of invalidating the assumptions licensees themselves have made in their plant-specific IPEs.

Licensees may not have thoroughly considered the safety (risk) aspects of doing more on-line maintenance. Some licensees have used the concept of division or train outages to ensure that they do not have a loss of system function. In the extreme, this could result in all of the equipment in a division being out of service at a time with unexamined risk consequences, while the licensee is in literal compliance with its plant's technical specifications. For example, one facility that used a division or train approach had planned to take out of service the following equipment: the B AFW pump, the B Battery charger, the B service water pump, the B RHR pump, and the B charging pump. Because redundant train equipment was available, no LCO was exceeded. However, in the event of a design-basis transient, such as a loss of offsite power precipitated by maintenance or instrumentation calibration activities associated with non-safety-related equipment in the switchyard, the plant would be in a configuration with significant risk implications due to the diminished capability to remove decay heat at a high pressure. This is an example of maintenance simultaneously increasing the probability of an initiating event, in this case the loss of offsite power, and diminishing the plant's capability to mitigate the event.

There is a clear link between effective maintenance and safety with regard to such issues as the number of plant transients and challenges to safety systems and the associated need to maximize the operability, availability, and reliability of equipment important to safety. In many cases, the only plant changes needed to reduce the probability of core damage are procedure changes. An example at one plant included staggering the quarterly tests of the station batteries to reduce the probability of common-cause failures of the dc power supplies.

4.11.4.4 Maintenance Rule

The maintenance rule, 10CFR50.65, becomes effective in July of 1996. One objective of the rule is to monitor the effectiveness of maintenance activities at the plants for safety-significant plant equipment in order to minimize the likelihood of failures and events caused by the lack of effective maintenance. Another objective of the rule is to ensure that safety is not degraded when maintenance activities are performed. The rule requires all nuclear power plant licensees to monitor the effectiveness of maintenance activities at their plants. The rule provides for continued emphasis on the defense-in-depth principle by including selected balance-of-plant (BOP) structures, systems, and components (SSCs); integrates risk consideration into the maintenance process; establishes an enhanced regulatory basis for inspection and enforcement of BOP maintenance-related issues; and gives a strengthened regulatory basis for ensuring that the progress achieved is sustained in the future. The maintenance rule is a results-oriented, performance-based rule. A results-oriented rule places a greater burden on the licensee to develop the supporting details needed to implement the rule, as opposed to that necessary for compliance with a traditional prescriptive, process-oriented regulation.

The maintenance rule consists of three parts: (1) goals and monitoring, (2) effective preventive maintenance, and (3) periodic evaluations and safety assessments. The scope of the rule includes safety-related structures, systems, and components that are relied upon to remain functional during and following design-basis events to ensure reactor coolant pressure boundary integrity, reactor shutdown capability, and the capability to prevent or mitigate the consequences of accidents, and those non-safety-related SSCs (1) that are relied upon to mitigate accidents or transients or are used in emergency operating procedures (EOPs), (2) whose failure could prevent safety-related SSCs from fulfilling their intended functions, or (3) whose failure could cause a scram or safety system actuation.

The rule requires that licensees monitor the performance or condition of certain structures, systems and components (SSCs) against licensee-established goals in a manner sufficient to provide reasonable assurance that those SSCs will be capable of performing their intended functions. Such monitoring would take into account industry-wide operating experience. The extent of monitoring may vary from system to system, depending on the contribution to risk. Some monitoring at the component level may be necessary; most of the monitoring could be done at the plant, system, or train level. Monitoring is not required where it has been demonstrated that an appropriate preventive maintenance program is effectively maintaining the performance of an SSC. Each licensee is required to evaluate the overall effectiveness of its maintenance activities at least every refueling cycle, again taking into account industry-wide operating experience, and to adjust its programs where necessary to ensure that the prevention of failures is appropriately balanced with the minimization of unavailability of SSCs. Finally, in performing monitoring and maintenance activities, licensees should assess the total plant equipment that is out of service and determine the overall effect on the performance of safety functions.

In June of 1995, the NRC published a report (NUREG-1526, "Lessons Learned from Early Implementation of the Maintenance Rule at Nine Nuclear Power Plants") which documents methods, strengths, and weaknesses found with the implementation of the rule at nine plant sites. These licensees implemented the rule using the guidance in NUMARC 93-01, "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants," which the NRC has endorsed in Regulatory Guide 1.160. Most licensees were thorough in determining which SSCs are within the scope of the rule. Some licensees incorrectly failed to classify a few non-safety-related systems as being within the scope of the rule. These systems included control room annunciators, circulating water systems, reactor coolant pump vibration monitoring systems, extraction steam systems, condenser air removal systems, screen wash water systems, generator gas systems, and turbine lubricating oil systems.

The rule requires that reliability goals be established commensurate with safety (risk). In determining which SSCs are risk significant, the typical licensee uses an expert panel consisting of a multidisciplinary team of PRA, operations, and systems experts in a working group format. The panel uses deterministic and operational experience information to complement PRA or IPE insights (importance measures) to establish the relative risk significance of SSCs. The risk determination is then used when setting goals and monitoring as required by the rule. The rule requires that appropriate corrective action shall be taken when the performance or condition of an SSC does not meet established goals. Many licensees have assigned the task of determining the root cause and developing corrective action to the responsible system engineer at the site; at some sites the expert panel participates in the process. The relative risk significance of SSCs must be reevaluated based on new information, design changes, and plant modifications.

The rule addresses preventive maintenance activities in the following manner: "adjustments shall be made where necessary to ensure that the objective of preventing failures of [SSCs] through maintenance is appropriately balanced against the objective of minimizing the effect of monitoring or preventive maintenance on the availability of [SSCs]." In other words, the unavailability of SSCs must be balanced with their reliability. Various methods are being implemented by licensees to perform these evaluations. For example, unavailability and reliability can be evaluated and balanced as an integral part of monitoring against performance criteria, taking into account performance history, preventive maintenance activities, and out-of-service times when developing the performance criteria. SSCs rendered unavailable because of preventive maintenance can be trended and evaluated, and adjustments can be made where necessary to balance the unavailability with reliability. In addition, the risk contribution associated with the unavailability of the system caused by preventive maintenance activities and the risk contribution associated with the reliability of the SSC can be calculated and then used to evaluate adjustments needed to balance the contribution from each source to ensure consistency with PRA or IPE evaluations. A fourth method involves using the PRA to determine values for unavailability and reliability which, if met, would ensure that certain threshold core damage frequency values would not be exceeded, and then establish performance criteria in accordance with the resulting unavailability and reliability values.

The rule requires that when performing monitoring and preventive maintenance activities, an assessment of the total plant equipment that is out of service should be considered to determine the overall effect on performance of safety functions. As expected by the results- or performance-oriented nature of the rule, various methods are being developed and implemented by licensees to fulfill this requirement. One method is a matrix approach, which involves listing preanalyzed configurations to supplement existing procedural guidance for voluntary on-line maintenance. The list of preanalyzed configurations is developed using importance measures to rank configurations according to risk. The equipment out-of-service matrix includes preanalyzed combinations of out-of-service equipment. A multilevel approach is then used to either (1) permit the concurrent activities, (2) require further evaluation, or (3) forbid the performance of the activities in parallel. A simplified example of an equipment out-of-service matrix is shown in Figure 4.11-16. Although the matrix approach is simple to use, it defines a limited number of combinations and may not address all operational situations and may unnecessarily limit operational flexibility.

Another method of monitoring the safety (risk) impact of plant configuration involves using the plant IPE to evaluate the changes in the core damage frequency resulting from equipment outages. In Figure 4.11-17, the core damage frequency was calculated for each day, based on the plant configuration that existed at the time, and plotted against time. This plant actually operated during the charted time period more conservatively than in its IPE, since the time-averaged core damage frequency, based on the actual plant configurations, was lower than the core damage frequency calculated in accordance with the IPE methodology. The "spikes" in core damage frequency correspond to periods of more risk-intensive configurations. Using this method in the predictive mode, the analysis of changes in the core damage frequency would be done during the maintenance planning and scheduling process. The maintenance schedule would be adjusted to minimize significant spikes in the core damage frequency. Figure 4.11-18 is a similar example from a different plant. This type of configuration control analysis is also being used at some foreign plants as the basis for risk-based technical specifications. In Figure 4.11-19, the magnitude of the projected increase in core damage frequency determines the amount of time the plant is allowed to be in the analyzed configuration. For example, if the calculated increase in core damage frequency is a factor of 10 or less above the baseline, the allowed duration in that configuration is 30 days; if the calculated increase is between a factor of 10 and a factor of 30 above the baseline, the allowed duration is 3 days. If the calculated increase in core damage frequency is greater than a factor of 30 above the baseline, then the configuration is not allowed.

Some licensees have implemented or are considering computer-based safety (risk) monitors that will calculate and display the risk changes associated with changes in plant configuration. Maintenance planners using the system in the predictive mode, or operators using the system on-line in real time, would be required by plant procedures to take predetermined actions and/or initiate further evaluations based on the magnitude of any indicated increase in risk (decrease in safety margin) due to a change in plant configuration or operating condition. In order for this type of system to be used for other than full power operating conditions, development and implementation of PRA models for shutdown plant conditions would be necessary.

4.11.4.5 Inspection of Configuration Management

The processes used by the licensees to schedule and plan on-line maintenance should ensure that maintenance and testing schedules are appropriately modified to account for degraded or inoperable equipment. The following are examples of questions that should help to determine the operations/maintenance level of familiarity with the process employed by a licensee in managing its scheduled maintenance activities. When planning on-line maintenance:

- Does the licensee take probabilistic risk insights into account?
- Does the licensee allow multiple train outages?
- How does the licensee take into account component and system dependencies?
- How does the licensee assure that important combinations of equipment needed for accident mitigation are not unavailable at the same time?
- By what process does the licensee determine the procedures and testing to emphasize in minimizing component unavailability and reducing the potential for accident or transient initiation, including the impact of maintenance activities involving non-safety-related equipment?
- How does the licensee determine the maxi-

mum amount of time to allow for the maintenance and how does it determine the risk associated with the decision?

- At any given time, how much planned maintenance is in progress and how is it coordinated to minimize risk?
- Are there occurrences of scheduled maintenance activities that simultaneously, or within a short period of time, impact two or more of the risk factors discussed in section 4.11.4.3?

Specific guidance and inspection requirements for maintenance activities can be found in the NRC Inspection Manual, chapter 62700. Attachment I contains an example of an inspection report that includes various items related to the inspection of risk and configuration management:

- IPE results were used to focus the inspectors' attention on the emergency switchgear ventilation, the loss of which was identified by the IPE as the initiator of the top-ranked sequence contributing to core damage frequency (cover letter, Notice of Violation, and section 3.1.2 of the inspection report).

- The associated violation regarding the white control power light for the emergency switchgear ventilation fans was cited against 10CFR50, Appendix B, Criterion XVI, "Corrective Actions." After July, 1996, this type of violation could be cited against the maintenance rule, 10CFR50.65.

- Section 4.4 of the report discusses the fact that the technical specifications allow certain configurations of plant equipment involving auxiliary feedwater pumps and high head safety injection pumps that could potentially place the plant in an unanalyzed condition.

This report illustrates how rigorous implementation of risk-based inspection techniques and insights with regard to the plant's configuration management and on-line maintenance practices can identify and resolve safety-significant issues, thereby reducing risk and improving safety.

4.11.5 Summary

Deterministic approaches to regulation consider a set of challenges to safety and determine how those challenges should be mitigated. A probabilistic approach to regulation enhances and extends the traditional deterministic approach by (1) allowing consideration of a broader set of potential challenges to safety, (2) providing a logical means for prioritizing these challenges based on risk significance, and (3) allowing consideration of a broader set of resources to defend against these challenges.

Licensees are increasing the amount and frequency of maintenance performed during power operation. Licensees' expansion of the on-line maintenance concept without thoroughly considering the safety (risk) aspects raises significant concerns. The maintenance rule is being implemented to ensure that safety is not degraded during the performance of maintenance activities. The rule requires all nuclear power plant licensees to monitor the effectiveness of maintenance activities.

The attached inspection report's content reinforces some of the concepts discussed in this section, such as risk-informed inspections (using IPE results to prioritize inspection activities - see section 3.1.2 of the inspection report) and maintenance rule applications (same section, which discusses maintenance trending, etc), and plant configurations which are allowed by the technical specifications but put the plant in an undesirable (unsafe/unanalyzed) condition (see section 4.4 of the inspection report).

4.11.6 References

1. "Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants" (WASH-1400), NUREG-75/014, U.S. Nuclear Regulatory Commission, Washington, DC, October 1975.

2. "Risk Assessment Review Group Report to the U.S. Nuclear Regulatory Commission," NUREG/CR-0400, September 1978.

3. "Report of the President's Commission on the Accident at Three Mile Island," J.G. Kemeny et al., October 1979.

4. "Three Mile Island - A Report to the Commissioners and to the Public," NUREG/CR-1250, Vol. 1, January 1980.

5. "Interim Reliability Evaluation Program Procedures Guide," NUREG/CR-2728, U.S. Nuclear Regulatory Commission, Washington, DC, January 1983.

6. "PRA Procedures Guide," NUREG/CR-2300, U.S. Nuclear Regulatory Commission, Washington, DC, January 1983.

7. "Probabilistic Risk Assessment Reference Document," NUREG-1050, U.S. Nuclear Regulatory Commission, Washington, DC, September 1984.

8. "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," NUREG-1150, U.S. Nuclear Regulatory Commission, June 1989.

9. "Individual Plant Examination for Severe Accident Vulnerabilities," Generic Letter No. 88-20, U.S. Nuclear Regulatory Commission, Washington, DC, November 1988.

10. "Fundamentals of PRA," Idaho National Engineering Laboratory, Idaho Falls, ID, January 1990.

11. "Analysis of Core Damage Frequency: Internal Events Methodology," NUREG/CR-4550, Vol. 1, Rev. 1, SAND86-2048, Sandia National Laboratories, Albuquerque, NM, January 1990.

12. "Fault Tree Handbook," NUREG-0492, U.S. Nuclear Regulatory Commission, Washington, DC, January 1981.

13. "Evaluation of Station Blackout Accidents at Nuclear Power Plants - Technical Findings Related to Unresolved Safety Issue A-44," NUREG-1032, U.S. Nuclear Regulatory Commission, Washington, DC, June 1988.

14. "Anticipated Transients Without Scram for Light Water Reactors," NUREG- 0480, Vol. 1, U.S. Nuclear Regulatory Commission, Washington, DC, April 1978.

15. "Study of the Value and Impact of Alternative Decay Heat Removal Concepts for Light Water Reactors," NUREG/CR-2883, Vol. 1,2,3, U.S. Nuclear Regulatory Commission, Washington, DC, June 1985.

16. "PRA Applications Program for Inspection at ANO-1," NUREG/CR-5058, U.S. Nuclear Regulatory Commission, Washington, DC, March 1988.

17. "Insights on Plant Specific Unique and/or Important to Safety Features Identified from 72 IPEs for 106 BWR and PWR Units," U.S. Nuclear Regulatory Commission, Washington, DC, July 1995.

18. "Handbook of Methods for Risk-Based Analyses of Technical Specifications,"

NUREG/CR-6141, December 1994.

19. "Lessons Learned from Early Implementation of The Maintenance Rule at Nine Nuclear Power Plants," NUREG-1526, U.S. Nuclear Regulatory Commission, Washington, DC, June 1995.

20. "Individual Plant Examination: Submittal Guidance," NUREG-1335, U.S. Nuclear Regulatory Commission, Washington, DC, August 1989.

21. "Perspectives on Reactor Safety," NUREG-CR-6042, SAND93-0971, Sandia National Laboratories, Albuquerque, NM, March 1994.

22. NRC Inspection Report Nos. 50-334/94-24 and 50-412/94-25, November 1994.

Table 4.11-1 INSIGHTS FROM REVIEW OF PLANT IPEs

Insight	Description	Applicability
Additional Nitrogen Supply	A backup nitrogen supply can usually reduce calculated core damage frequency (CDF) caused by loss of pneumatic power supply to important plant components such as safety/relief valves and main steam isolation valves inside containment.	BWR and PWR
Gas Turbine Generators	Gas turbines can be an alternate ac power source to keep the plant functioning during a station blackout (SBO) or loss of offsite power (LOSP) during which even the emergency diesel generators (DGs) fail to start.	BWR and PWR
Containment Venting Capability	Containment venting can prevent core damage and provide containment overpressure protection under certain severe accident scenarios. Loss of containment heat removal has been identified in many BWR PRAs as a significant contributor to CDF. A hardened vent provides a means of removing heat from the containment, independent of the RHR and plant service water systems.	BWR
Additional Diesel Generators	Increased redundancy and diversity in electrical power supply systems substantially reduces the likelihood of certain accident events. Several IPEs identified the need to perform maintenance and testing of the DGs on a separate schedule using different personnel, and the need for operators to be thoroughly trained in its use.	BWR and PWR
Bleed and Feed	Most PWRs have bleed and feed (once-through core cooling) capability. Bleed and feed requires high pressure injection pump(s) and PORVs.	PWR

Table 4.11-1	INSIGHTS FROM REVIEW OF PLANT IPEs	(continued)
Cross-tying of Firewater System	A residual heat removal system/firewater cross-tie provides the capability for low pressure injection during most events in which normal injection systems are unavailable.	BWR and PWR
Cross-tying of Multi-Unit Safety Systems (Auxiliary Feedwater, Component Cooling Water, Service Water, Control RoomHVAC, Electrical Power)	At multi-unit sites, the ability to cross-tie a safety system from the opposite unit affords additional redundancy in that system. Redundant electrical power and air supplies via cross-ties assure reliable system initiation and operation.	Multi-unit PWRs and BWRs
Increasing Battery Capacity to Cope with Station Blackouts	The majority of BWR and PWR units have 8-hour battery capacities. This relatively large capacity provides significant time for recovery in the event of an SBO. CDF may be reduced by increasing battery capacity for plants that have less than 8-hour battery capacities.	BWR and PWR
Reliability of Air-operated Valves vs. Motor-operated Valves	General data indicate that the failure probability for air-operated valves (AOVs) is lower than that for motor-operated valves. In addition, AOVs normally fail to their accident positions, reducing the vulnerability to SBO upon the loss of air or loss of power.	BWR and PWR
Reactor Coolant Pump Modifications	Loss of component cooling water and station blackout are initiators for the failures of RCP seals, which result in seal LOCAs. The use of qualified O-rings and/or durable pump seals reduces the probability of seal LOCAs.	PWR
Load Shedding	Implementation of dc load shedding procedures may extend dc power to 14 hours or greater to cope with a station blackout.	BWR and PWR

Deterministic Analysis

- Standard good engineering practices, calculations, and judgements

Defense-In-Depth

- Multiple fission product barriers
- Redundancy
- Diversity
- Single Failure Criteria
- Worst Case Assumptions

Figure 4.11-1 Deterministic Analysis

Probabilistic Risk Assessment

- What can go wrong?
- Likelihood?
- Consequences?

Results

- Dominant Contributors
- Dominant Accident Sequences
- Importance Measures

Figure 4.11-2 Probabilistic Risk Assessment

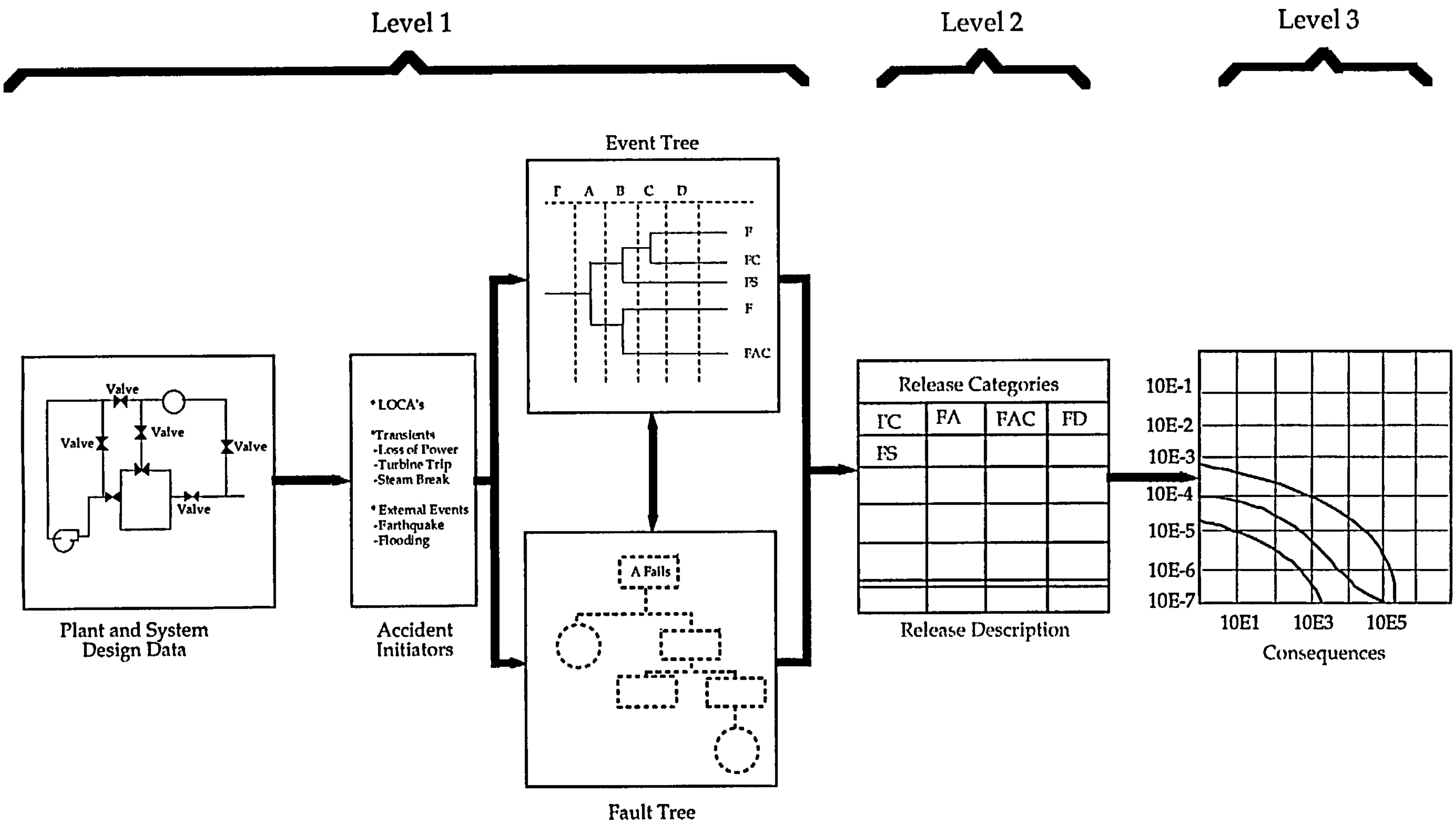


Figure 4.11-3 Elements of PRA

History

1975 Reactor Safety Study (WASH-1400)

1980 Severe Accident Risks: An Assessment An Assessment for Five U.S. Nuclear Power Plants (NUREG-1150)

1985 Severe Accident Policy

1988 Individual Plant Examination (IPE) Program (Generic Letter 88-20)

1993 Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations (NUREG-6143)

Figure 4.11-4 Historical Perspective

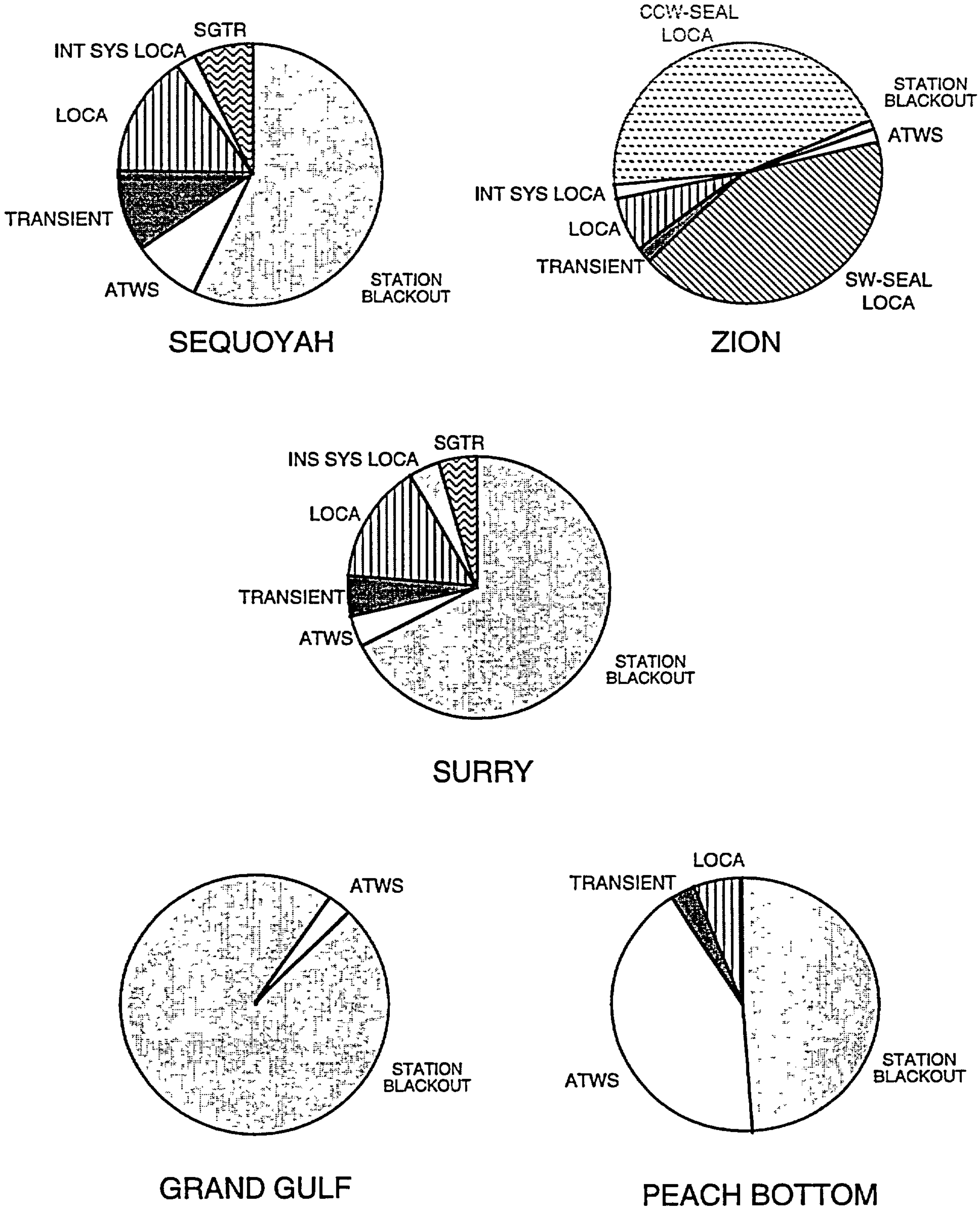
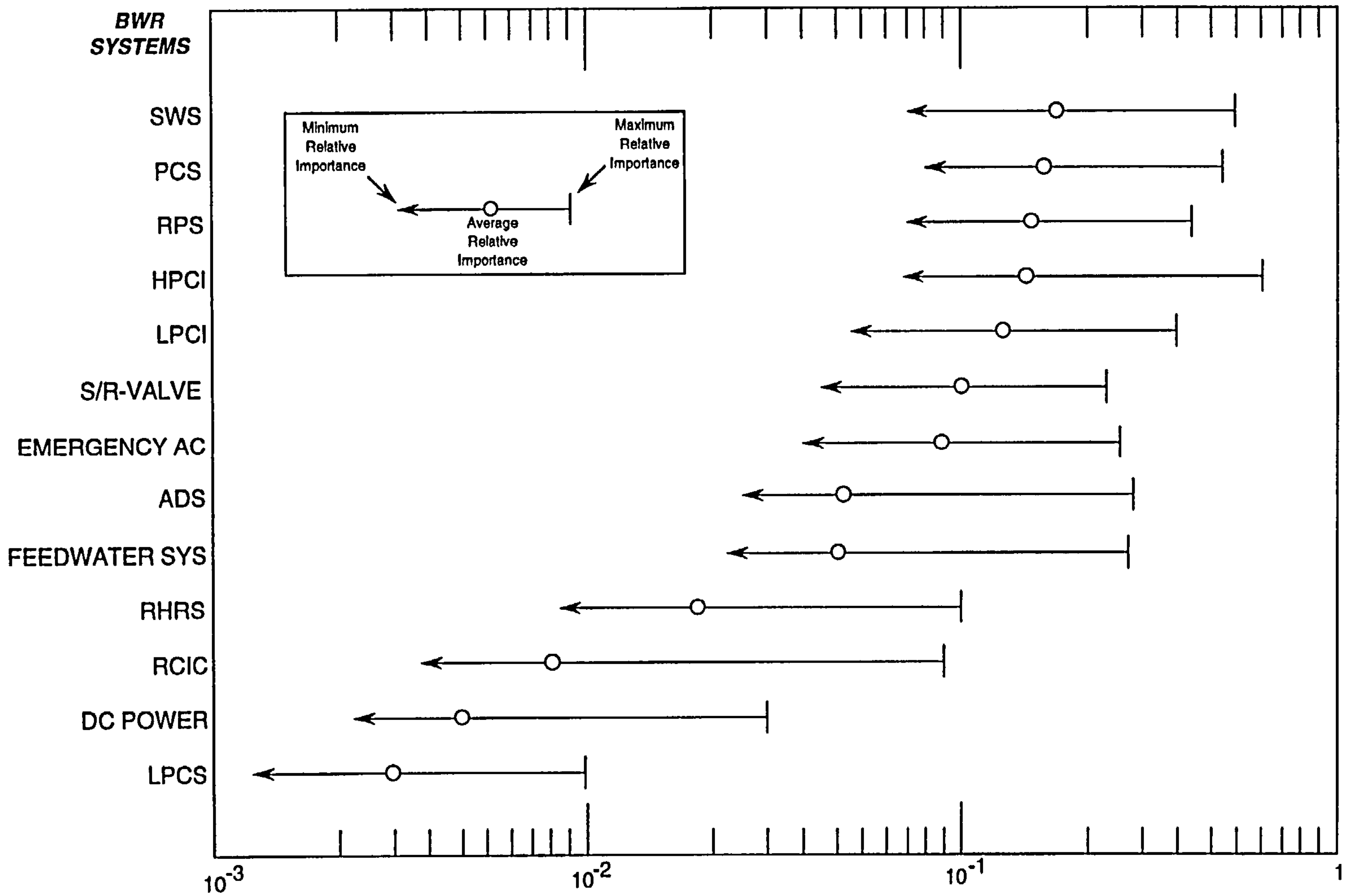


Figure 4.11-5 Major Contributors To Core Damage By Accident Types



Relative importance of BWR Systems considering dominant accident sequences from 15 PRAs

Source NuReg-1050

Figure 4.11-6 Relative Importance Factors

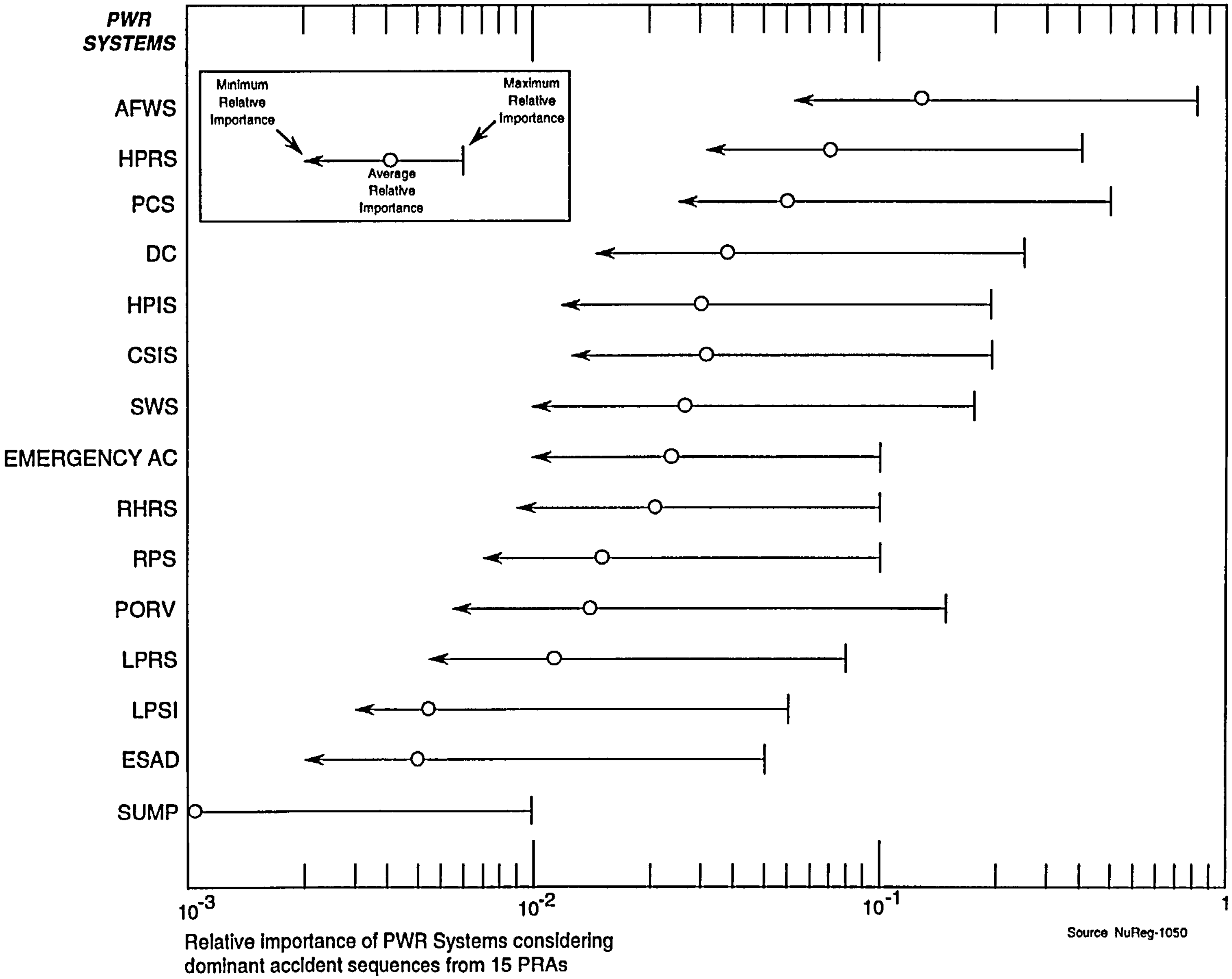


Figure 4.11-7 Relative Importance Factors

Risk-Based Regulation

A regulatory approach in which insights derived from PRA are used in combination with deterministic and engineering analyses to focus licensee and regulatory attention on issues commensurate with their importance to safety.

- ATWS Rule (10CFR50.62)
- Auxiliary Feedwater System Reliability
- Blackout Rule (10CFR50.63)
- Backfit (10CFR50.109)
- Risk-Based Inspection

Figure 4.11-8 Risk Based Regulation

PRA Policy Statement (August 16, 1995)

- Increased use of PRA in reactor regulatory matters should be implemented to the extent supported by state of the art in PRA methods and data and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy.
- PRA should be used to reduce unnecessary conservatism associated with current regulatory requirements. Where appropriate, PRA should be used to support additional regulatory requirements.
- PRA evaluations in support of regulatory decisions should be as realistic as possible and appropriate supporting data should be publicly available.
- Uncertainties in PRA evaluations need to be considered in applying the Commission's safety goals for nuclear power plants.

Figure 4.11-9 PRA Policy Statement

PRA Implementation Plan

- Agency-Wide Plan to Implement the PRA Policy Statement
- Includes both on-going and new PRA related activities
- Encourages risk-based initiatives from licensees

PRA Applications

- Graded Quality Assurance
- Inservice Testing
- Inservice Inspection
- Technical Specifications
- Maintenance Rule
- IPE Insights
- Reliability Data Rule (proposed)

Figure 4.11-10 PRA Implementation Plan

Risk Management

A means of prioritizing resources and concerns to control the level of safety (risk).

Configuration Management

Managing the configuration of plant systems to control the level of safety (risk).

Figure 4.11-11 Risk and Configuration Management - Definitions

0196-X

RISK MANAGEMENT FACTORS

$$Risk = P_i \times P_m \times P_c$$

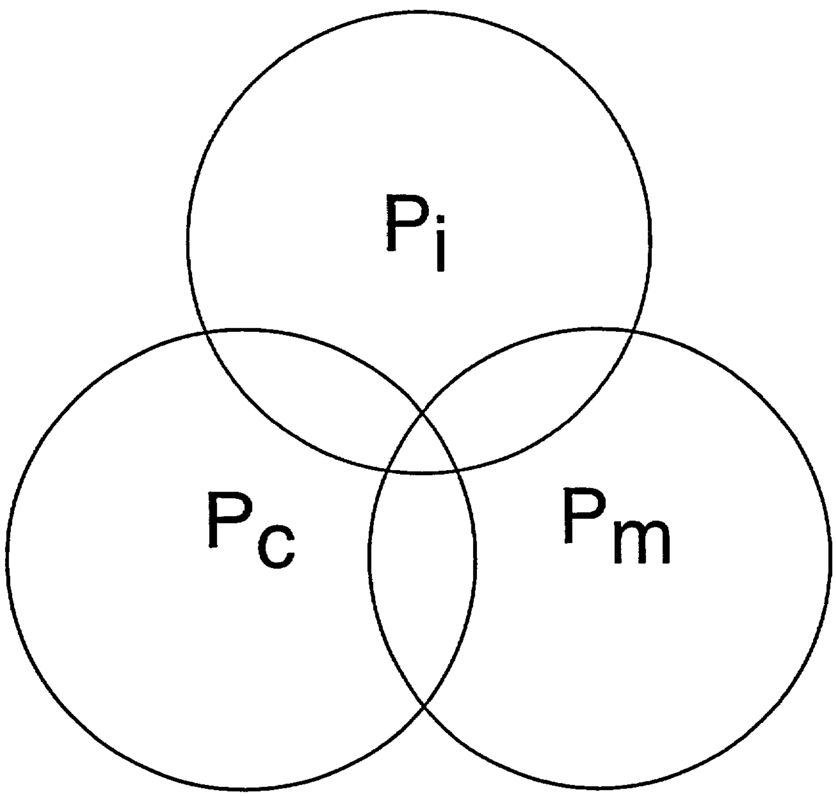


Figure 4.11-12 Risk Management Factors

Maintenance Rule (10CFR50.65)

Effective July 1996

Overall objective of rule is to monitor the effectiveness of maintenance activities...for safety significant plant equipment...in order to minimize the likelihood...of failures and events...caused by the lack of effective maintenance.

- Goals and Monitoring
- Effective Preventive Maintenance
- Periodic Evaluations and Safety Assessments.

Figure 4.11-13 Maintenance Rule - Objectives

Scope

- Safety-related structures, systems, and components that are relied upon to remain functional during and following design basis events to ensure RCS pressure boundary integrity, reactor shutdown capability, safe shutdown capability, and the capability to prevent or mitigate the consequences of accidents

- non-safety-related SSCs

  (1) that are relied upon to mitigate accidents or transients or are used in emergency operating procedures (EOPs),

  (2) whose failure could prevent safety-related SSCs from fulfilling their intended functions, or

  (3) whose failure could cause a scram or safety system actuation.

Figure 4.11-14 Maintenance Rule - Scope

Configuration Risk Monitoring Methods

- Matrix approach
  (pre-analyzed configurations)

- CDF impact analysis

- Safety (risk) monitor

Figure 4.11-15 Configuration Risk Monitoring Methods

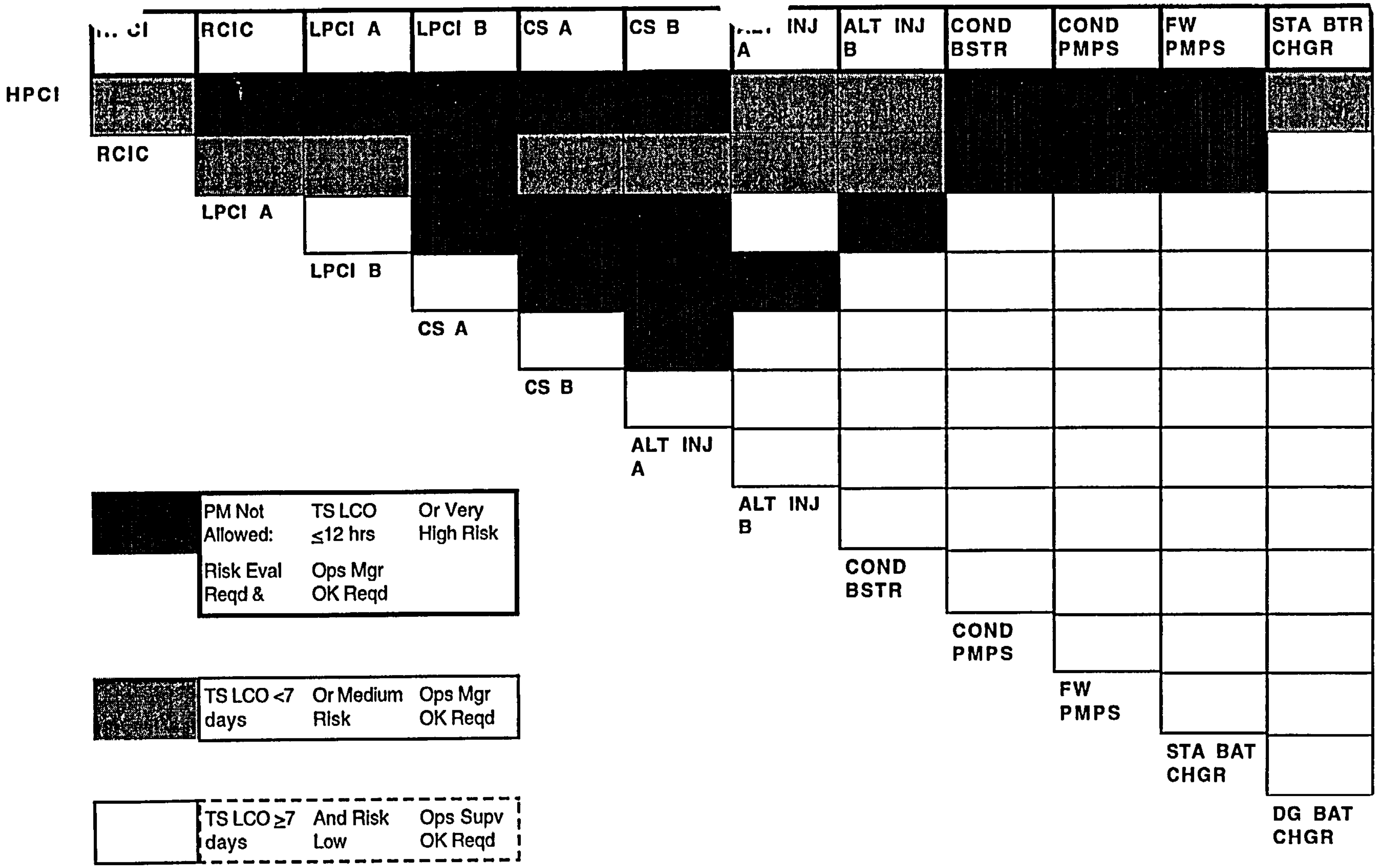


Figure 4.11-16 Preventive Maintenance Equipment Out-Of-Service Matrix

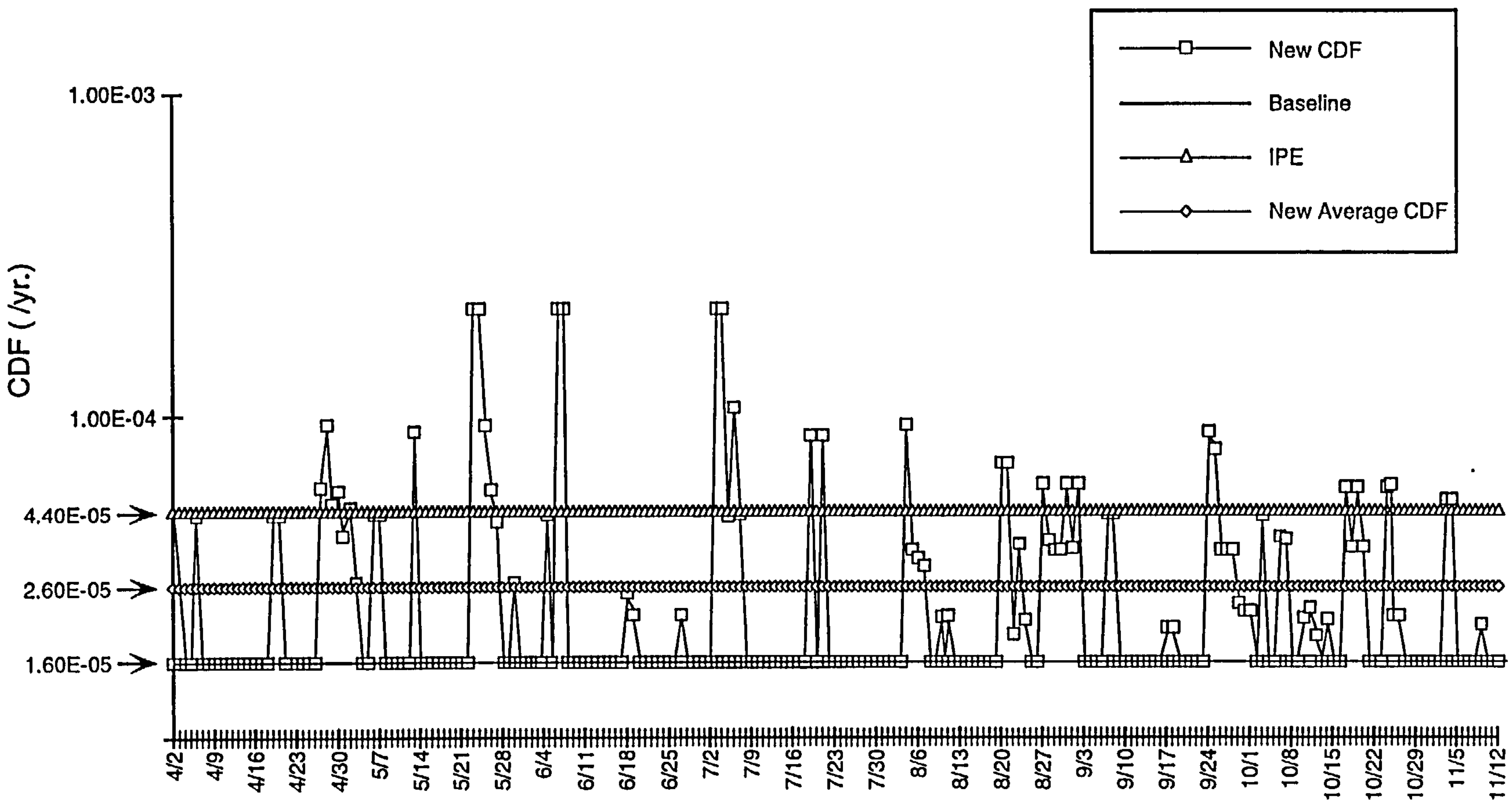
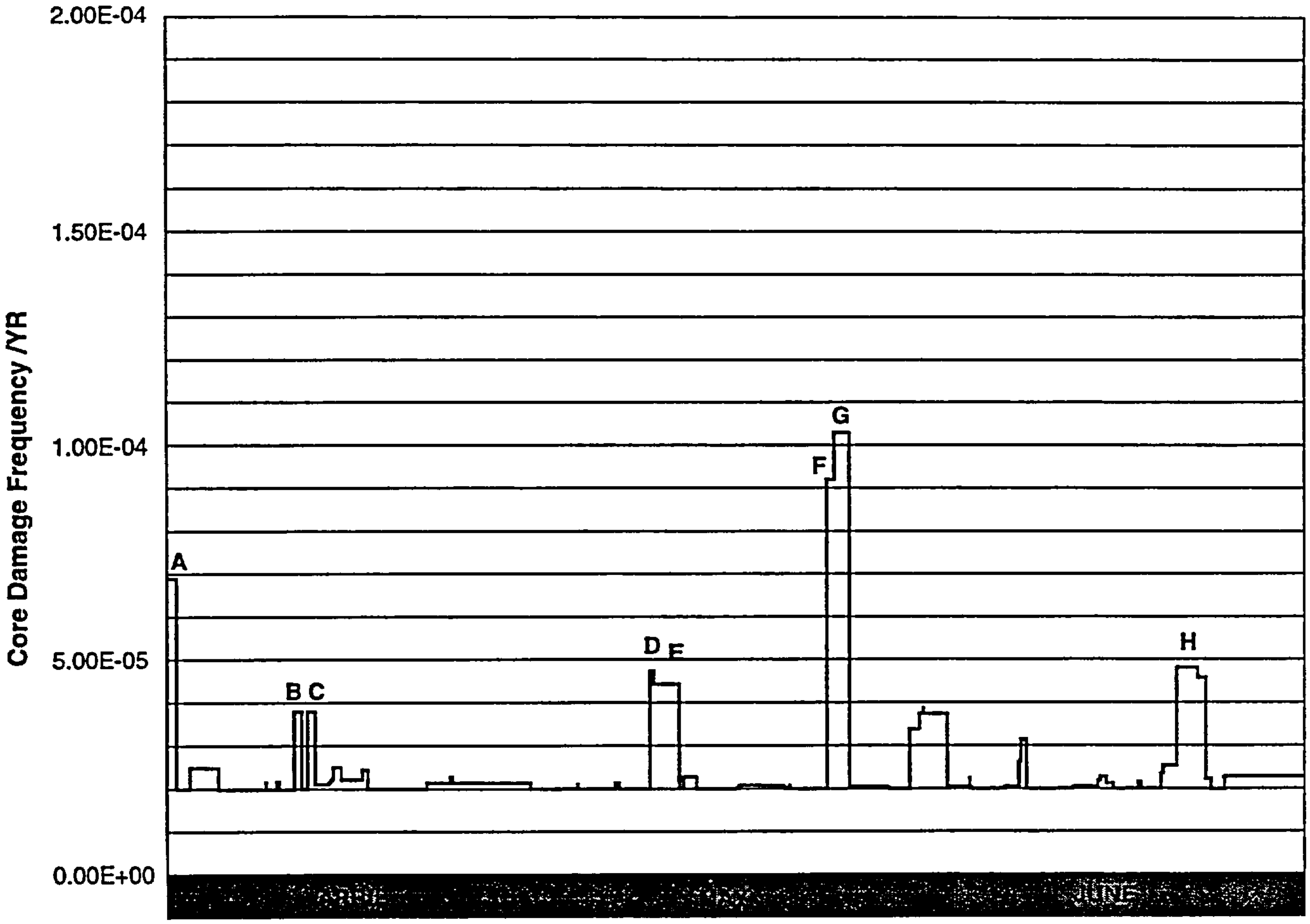


Figure 4.11-17 Risk Monitoring

0196-X

UNIT 2 INSTANTANEOUS RISK GRAPH



(A) Emergency Chilled Water Pump P162 Control Transformer Replacement
(B) Train B Cold Leg Injection Valves 2HV9329/HV9323 Transformer Replacement
(C) Train B Cold Leg Injection Valves 2HV9326/HV9332 Transformer Replacement
(D) Diesel Generator 2G003 Annual Maintenance and HPSI 2P019 Preventive Maint.
(E) Diesel Generator 2G003 Annual Maintenance and SWC 2P114 Preventive Maint.
(F) AFW Pump P141 Preventive Maintenance
(G) AFW Pump P141 Preventive Maintenance and PPS Testing
(H) Diesel Generator 2G002 Annual Maintenance and SWC 2P112 Preventive Maint.

Core damage frequency (CDF) calculated for Mode 1 operations only.
Average CDF for 3 month period = 2.4E-05/yr.

Figure 4.11-18 Risk Monitoring Predictive

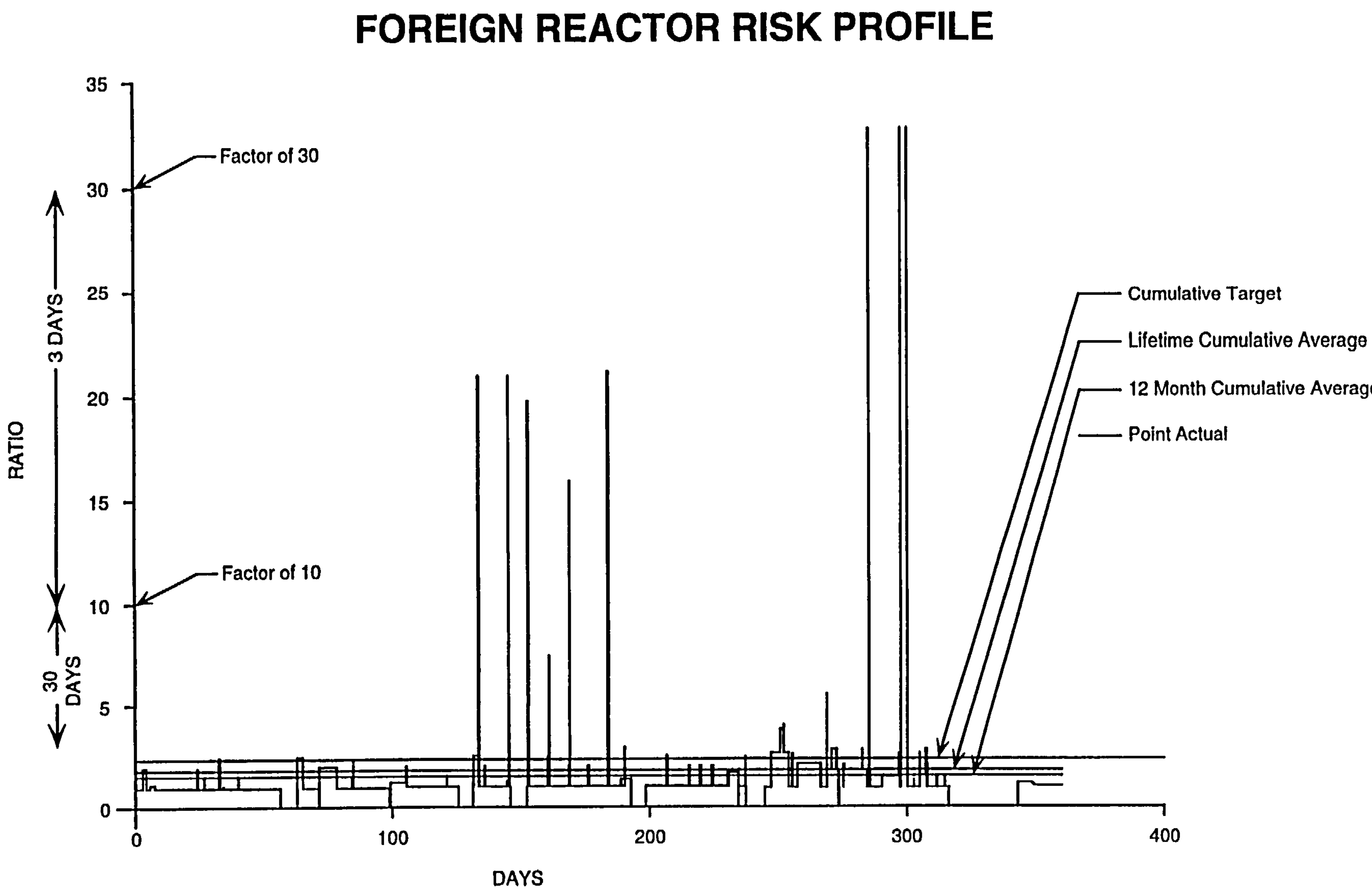


Figure 4.11-19 Risk Profile for Allowed Outage Time Determination

0196-X

Attachment 1 - NRC Inspection Report Nos. 50-334/94-24 AND 50-412/94-25
Chapter 4.11
Risk Management

ENCLOSURE 1

NOTICE OF VIOLATION

Duquesne Light Company
Beaver Valley Power Station, Unit 2

Docket Nos. 50-412
License Nos. NPF-73

During an NRC inspection conducted between October 11 and November 14, 1994, one violation of NRC requirements was identified. In accordance with the "General Statement of Policy and Procedure for NRC Enforcement Actions," 10 CFR Part 2, Appendix C, the violation is listed below:

10 CFR Part 50, Appendix B, Criterion XVI, "Corrective Actions," states, in part, that measures shall be established to assure that conditions adverse to quality, such as failures, malfunctions, deficiencies, deviations, defective material and equipment, and non-conformances are promptly identified and corrected.

Contrary to the above, as of October 21, 1994, established measures did not assure that conditions adverse to quality were promptly identified and corrected. Specifically, the investigations of an unusually dim white control power light for emergency switchgear ventilation fans 2HVZ-FN261A on October 30, 1993, and 2HVZ-FN261B on September 24, 1994, failed to identify that the standby fan would not start if called upon following the loss of the running fan except when started by the emergency diesel sequencer. Equipment maintenance history was not used to identify that a trend of similar problem descriptions of a dim white control power light has existed since 1989.

This is a Severity Level IV violation (Supplement I).

Pursuant to the provisions of 10 CFR 2.201, Duquesne Light Company is hereby required to submit a written statement or explanation to the U.S. Nuclear Regulatory Commission, ATTN: Document Control Desk, Washington, D.C. 20555 with a copy to the Regional Administrator, Region I, and a copy to the NRC Resident Inspector at the facility that is the subject of this Notice, within 30 days of the date of the letter transmitting this Notice of **Violation 94-25-01**. This reply should be clearly marked as a "Reply to a Notice of Violation" and should include for each violation: (1) the reason for the violation, or, if contested, the basis for disputing the violation, (2) the corrective steps that have been taken and the results achieved, (3) the corrective steps that will be taken to avoid further violations, and (4) the date when full compliance will be achieved. If an adequate reply is not received within the time specified in this Notice, an order or a Demand for Information may be issued to show cause why the license should not be modified, suspended, or revoked, or why such other action as may be proper should not be taken. Where good cause is shown, consideration will be given to extending the response time.

Dates at King of Prussia, Pennsylvania
this 29th day of November, 1994

in developing their EAL scheme but may not use portions of both methodologies." The staff stated in Emergency Preparedness Position on Acceptable Deviations from Appendix 1 of NUREG-0654 based upon the Staff's regulatory analysis of NUMARC/NESP-007 that it recognizes that licensees who continue to use EALs based upon NUREG-0654 could benefit from the technical basis from EALs provided in NUMARC/NESP-007. However, the staff also recognized that the classification scheme must remain internally consistent. Likewise, Licensees can benefit from guidance provided in NEI 99-01 without revising their entire EAL scheme. This is particularly true in regard to adopting guidance on EALs for cold shutdown and refueling modes of operation or for Independent Fuel Storage facilities. However, the licensee still needs to ensure that its EAL scheme remains internally consistent.

4.12.3 NUREG-0654

NUREG-0654/FEMA-REP-1 was published to provide a common reference and guidance source for:

- Nuclear facility operators as well as State and local governments in the development of radiological emergency response plans and preparedness in support of nuclear power plants.
- Federal Emergency management Agency (FEMA), Nuclear Regulatory Commission (NRC), and other Federal agency personnel engaged in the review of State and, Local government and licensee plans and preparedness.
- FEMA, NRC and other Federal agencies in the development of the National Radiological Emergency Plan.

NUREG-0654/FEMA-REP-1 was prepared as part of their responsibilities under the Atomic Energy Act, as amended, and the President's Statement of December 7, 1979, with the accompanying Fact Sheet. The responsibilities include development and promulgation of guidance to nuclear facility operators, State and local governments, in cooperation with other Federal agencies. The guidance included preparation of radiological emergency response plans and assessing the adequacy of such plans.

4.12.3.1 NUREG-0654/FEMA-REP-1, Appendix- 1

Appendix 1 of NUREG-0654/FEMA-REP-1, contains the Emergency Action Level Guidelines for Nuclear Power Plants. Within Appendix 1 four classes of Emergency Classification Levels (EAL) are established:

- Notification of Unusual Event
- Alert
- Site Area Emergency
- General Emergency

A graduation is provided to assure fuller response preparations for more serious indicators. The rationale for the notification and alert classes is to provide early and prompt notification of minor events which lead to more serious consequences given operator error or equipment failure or which might be indicative of more serious conditions which are not yet realized. The site area emergency class reflects conditions where some significant releases are likely or are occurring but where a core melt situation is not indicated based on current information. In this situation full mobilization of emergency personnel in the near site environs is indicated as well as dispatch of monitoring teams and associated communications. The general emergency class involves actual or imminent substantial core degradation or core melting with potential for loss of containment. The immediate action for this class is sheltering (staying inside) rather than evacuation until assessment can be made that (1) an evacuation is indicated and (2) an evacuation, if indicated, can be completed prior to significant release and transport of radioactive material to the affected areas.

Facility licensees have primary responsibility for accident assessment. This includes prompt action to evaluate any potential risk to the public inspections, the NRC will determine whether further NRC enforcement action is necessary to ensure compliance with NRC regulatory requirements.

In accordance with 10 CFR 2.790 of the NRC's "Rules of Practice," a copy of this letter, its enclosures, and your response will be placed in the NRC Public Document Room. Accordingly, your response should not, to the extent possible, include any personal privacy, proprietary, or safeguards information so that it can be released to the public and placed in the NRC Public Document Room.

The responses directed by this letter and the enclosed Notice are not subject to the clearance procedures of the Office of Management and Budget as required by the Paperwork Reduction Act of 1980, Pub. L. No. 96.511.

Your cooperation with us is appreciated.

Sincerely,

Original Signed By:

James C. Linville, Chief
Projects Branch No. 3
Division of Reactor Projects

Docket Nos. 50-334; 50-412

Enclosures:
1. Notice of Violation
2. NRC Inspection Report Nos. 50-334/94-24 and 50-412/94-25

cc w/encls:
G. S. Thomas, Vice President, Nuclear Services
T. P. Noonan, President, Nuclear Operations
L. R. Freeland, General Manager, Nuclear Operations Unit
K. D. Grada, Manager, Quality Services Unit
N. R. Tonet, Manager, Nuclear Safety Department
H. R. Caldwell, General Superintendent, Nuclear Operations
K. Abraham, PAO (2 copies)
Public Document Room (PDR)
Local Public Document Room (LPDR)
Nuclear Safety Information Center (NSIC)
NRC Resident Inspector
Commonwealth of Pennsylvania
State of Ohio

which technical specifications are exceeded and the capability of licensed operators to gain control and bring the indicators back to safe levels. Event-based ICs and EALs refer to discrete occurrences with potential safety significance such as a fire or severe weather. Barrier-based ICs and EALs utilize indications of the level of challenge to the principal barriers used to assure containment of radioactive materials within a nuclear plant. For the most important type of radioactive material, i.e., fission products, there are three principal barriers:

- Fuel cladding
- Reactor coolant system boundary
- Containment

In the NUMARC/NESP-007 methodology, the operating modes (power operation, startup, hot standby, hot shutdown, cold shutdown, refueling, and defueled) to which individual ICs apply are specified. As a plant moves from power operation through the decay heat removal process toward cold shutdown and refueling, barriers to the release of fission products may be reduced, instrumentation to detect symptoms may not be fully effective and partially disabling of safety systems may be permitted by technical specifications. For such operations, ICs and EALs tend to be event-based rather than symptom-based.

The ICs and EALs are divided into four "recognition categories" in NUMARC/NESP-007:

- A - Abnormal Rad Levels/Radiological Effluent
- F - Fission Product Barrier Degradation
- H - Hazards or Other Conditions Affecting Plant Safety
- S - System Malfunction

For recognition categories A, H, and S, ICs and associated EALs are developed for each emergency classification level. For these recognition categories, ICs are identified by a three character acronym. For example, AU2 is the second Unusual Event IC in the Abnormal Radiation Level recognition category and SS3 is the third Site Area Emergency IC in the System Malfunction recognition category.

For recognition category F, there are three ICs:

1. Loss or potential loss of the fuel clad barrier, and
2. Loss or potential loss of the RCS barrier.
3. Loss or potential loss of the containment barrier.

The EALs for each of these ICs depend on whether the reactor is a PWR or BWR. The emergency condition level is a function of the number (and extent) of fission product barrier degradation, as indicated below:

UNUSUAL EVENT	Any loss or potential loss of containment
ALERT	Any loss or any potential loss of either fuel clad or RCS
SITE AREA EMERGENCY	Loss of both fuel clad and RCS; or Potential loss of either; or Potential loss of either, and loss of any additional barrier
GENERAL EMERGENCY	Loss of two barriers and potential loss of the third barner

Table 4.12-6 provides an example of an emergency action level (EBD-S) bases document for system malfunction category SU5. The acronym SU5 is the fifth Unusual Event IC in the System Malfunction recognition category.

4.12.5 NEI 99-01 (NUMARC/NESP-007- Rev. 4)

Revision 4 to NUMARC/NESP-007 (NEI 99-01) presents the methodology for development of emergency action levels as an alternative to NRC/FEMA guidelines contained in Appendix 1 of NUREG-0654/FEMA-REP-1, Rev.2 "Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of nuclear Power Plants," October 1980 and 10 CFR 50.47 (a)(4). Revision 4 of NUMARC/NESP-007 enhances Revision 3 (NEI 97-03) by considering the system malfunction initiating conditions and example emergency action levels which address conditions that maybe

EXECUTIVE SUMMARY
Beaver Valley Power Station
Report Nos. 50-334/94-24 & 50-412/94-25

Plant Operations

Good operator performance was demonstrated during response to a loss of pressure in the control room temperature control air system, and to a blown fuse in the Unit 1 solid state protection system. Troubleshooting of a decrease in vacuum on the 2-1 emergency diesel generator was well planned and documented. Operators at Unit 1 demonstrated a strong questioning attitude when they identified a potential relationship between an out-of-service quench spray pump and net positive suction head to the recirculation spray pumps. However, the recirculation spray pumps were unnecessarily removed from service before it was determined that one quench spray pump will ensure adequate net positive suction head.

Maintenance

An unusually dim control power light for emergency switchgear ventilation fans led to identification of a deficiency with the control circuitry. Specifically, if the running fan was to fail for any reason, the standby fan could not auto-start or be manually started without first placing the failed fan control switch in "pull to lock" unless sequenced on by the emergency diesel sequencer. Previous troubleshooting efforts did not identify or correct this problem, and maintenance history trending was not used to identify the need for additional investigations of this control circuitry despite a history of work requests with a similar problem description. Additionally, operations and maintenance personnel, and the system engineer, were unaware that the licensee's Individual Plant Examination identified the loss of emergency switchgear ventilation as the top ranked initiating sequence contributing to core damage frequency. The failure to promptly identify the emergency switchgear ventilation control circuitry deficiency is a **violation** of 10 CFR 50, Appendix B, Criterion XVI, "Corrective Actions."

Operations personnel re-identified a previous deficiency associated with the SLCRS system that had not been repaired for almost three years. Good management attention has been subsequently focused on the timely repair of this deficiency. Test data showed that the system still would have performed its function. Corrective actions to address problems with the diesel speed sensing circuit and the rod control system were also appropriate.

Engineering

The licensee continued to demonstrate leadership in the nuclear industry through the identification of significant generic issues. Specifically, the licensee identified an AMSAC design deficiency which would have made the system inoperable if feedwater flow on one channel was outside its normal band, and issued a 10 CFR Part 21 notification concerning an anomaly with the test circuits on the Unit 1 solid state protection system. The AMSAC issue is still under evaluation for Part 21 applicability.

Development for Emergency Action Levels"

- Nuclear Energy Institute (NEI) submitted NEI 99-01, Methodology for Development of Emergency Action Levels

Onsite and Offsite emergency response plans must meet the standards that are listed in 10 CFR 50.47 in order for the staff to make a positive finding that there is reasonable assurance that adequate protective measures can and will be taken in the event of a radiological emergency. One of these standards, 10 CFR 50.47(b)(4), pertains to the development of emergency classification and actions level scheme. Section IV", Content of Emergency Plans", of Appendix E to 10 CFR Part 50 also contains requirements for the development and review of EALs.

TABLE OF CONTENTS

2.2 Loss of Control Room Temperature Control Air Pressure

On November 14, 1994, at 3:25 p.m., the plant operators at Unit 1 received a control room temperature control air pressure low alarm. The air system pressure was found at 15 psig. Normal system pressure is between 50 and 70 psig. The alarm response procedure refers the operators to the control room emergency habitability system technical specification (3.7.7.1) and Updated Final Safety Analysis Report (UFSAR) Section 9.13.4 "Main Control Area." After reviewing these references, the Shift Supervisor concluded that he could not be assured of operability of the Unit 1 control room supply and exhaust dampers. These dampers, VS-D-40-1A through D, have a flexible boot seal which provides for air-tight isolation of the control room during accident conditions. The control room temperature control air system supplies air to these seals. Consequently, at 4:10 p.m., it was identified that both Units 1 and 2 were required to enter Technical Specification 3.0.3, which requires action within 1 hour to initiate plant shutdown. Both units were in Mode 1 and both units began preparations for plant shutdown. The operators determined that the loss of air pressure was due to a stuck open automatic moisture blowdown valve. The valve was isolated and the low pressure alarm cleared at 4:27 p.m. The units exited Technical Specification 3.0.3 at 4:34 p.m. Neither unit progressed to the point of reducing power.

The inspectors reviewed this event and concluded that the operators took appropriate response actions. The inspectors did note that the event indicated a potential single failure vulnerability in the safety-related control room temperature control air system. The vulnerability is "potential" because the damper seals have backup accumulators and isolation check valves which may allow the seals to work even with a loss of pressure in the rest of the system. However, the accumulators and the check valves are apparently not tested to ensure this capability. The licensee was still evaluating this failure vulnerability when the report period ended.

2.3 Unit 1 Quench Spray Pump Maintenance

During a routine control room walkdown, the inspectors noted that the licensee had removed the Unit 1 `A' train recirculation spray and quench spray pumps from service. The pumps were taken out of service by a clearance for maintenance on the quench spray pump (oil leak repair). The inspectors asked why the recirculation spray pumps were included on the clearance. The inspectors found that the night-shift crew had a concern about net positive suction head to the recirculation spray pumps when removing a quench spray pump from service. Some of the flow from the quench spray pumps is diverted directly to the containment sump. This provides added cooling for the sump water to ensure adequate net positive suction head for the recirculation spray and low head safety injection pumps under all design basis conditions. The night-shift operators were concerned that removing one quench spray pump from service, while leaving all the recirculation spray pumps in service, might leave the opposite train recirculation spray pumps without sufficient net positive suction head.

3.0 MAINTENANCE (62703, 61726, 71707)

3.1 Maintenance Observations

The inspectors reviewed selected maintenance activities to assure that: the activity did not violate Technical Specification Limiting Conditions for Operation and that redundant components were operable; required approvals and releases had been obtained prior to commencing work; procedures used for the task were adequate and work was within the skills of the trade; activities were accomplished by qualified personnel; radiological and fire prevention controls were adequate and implemented; QC hold points were established where required and observed; and equipment was properly tested and returned to service.

The maintenance work requests (MWRs) listed below were observed and reviewed. Unless otherwise indicated, the activities observed and reviewed were properly conducted.

MWR 035464 No. 2 EDG Jacket Water Pressure Alarm Troubleshoot and Repair

See Section 3.2.2 of this report.

MWR 036230 Troubleshoot and Repair SSPS Alarms

On November 4, 1994, plant operators at Unit 1 received several intermittent alarms and indications associated with the solid state protection system (SSPS). The intermittent nature of the alarms told the operators that the problem was associated with only one channel of the SSPS (because of the multiplexing arrangement, a problem with only one channel of the SSPS will cause the indications to flash in and out). The problem was quickly isolated to a blown fuse in channel 1 of train `B' in the SSPS. The inspectors observed the licensee's efforts to verify and replace the fuse. The inspectors observed excellent coordination between the operations and maintenance personnel. Part of the maintenance included removing power from the affected channel of the SSPS. This evolution was very thoroughly researched and briefed. The Unit 1 Operations Manager reminded everyone of the importance of self-checking, and the pitfalls of haste. This was particularly appropriate since the plant entered a 6 hour Technical Specification action statement.

MWR 036371 Troubleshoot and Repair SSPS Intermittent Alarms

MWR 035759 Investigate Emergency Switchgear Ventilation Relay 162-HVZBB

MWR 036084 Emergency Switchgear Ventilation Fan 2HVZ-FN261A Troubleshooting

MWR 036084 Emergency Switchgear Ventilation Fan 2HVZ-FN261B Troubleshooting

MWR 036447 Blocking Diode Installation Per DCP 2124

MWRs 035759, 036084, 036084, and 036477 are discussed in Section 3.1.2.

162-HVZBB energized with the fan in a standby condition. The inspectors and licensee personnel physically verified that this relay was indeed energized. This relay should be de-energized when the fan is in standby. The consequence of this relay being energized is that fan 2HVZ-FN261B will not auto-start as designed upon loss of the `A' train fan. Operators would also be unable to manually start the `B' fan since relay 162-HVZBB is maintaining the "anti-pump" and trip coils of the fan breaker energized. The inspectors observed various fan manipulations which verified that the `B' fan would not auto start if a very dim white-light condition existed. It was possible to clear this locked-up relay and obtain a normal white control power light by first placing the control switch in "pull to lock," then back to auto. Some operators knew of this condition and considered it to be a "workaround." Current operating and alarm response procedures (fan auto-stop and high switchgear area temperature) did not specify the need for this control switch manipulation upon failure of the running fan. Further review of the fan start circuitry with relay personnel determined that both trains of fans would properly auto-start with the emergency diesel sequencer if called upon during a loss of power to the respective emergency bus.

The inspectors reviewed the maintenance history (since 1993) for both trains of emergency switch gear supply ventilation fans and noted that three recent MWRs were generated to investigate the dim white light condition. Each MWR is summarized below:

- MWR 015912 was opened on January 14, 1993, and worked on October 10, 1993, to investigate the dim white control power light for fan 2HVZ-FN261A. Since the control switch was in pull to lock during this maintenance, no problems were found and post maintenance testing verified proper fan operation.

- MWR 032143 was opened on June 11, 1994, to investigate the dim white control power light for fan 2HVZ-FN261A. This MWR was scheduled to be worked during the upcoming refueling outage.

- MWR 35001 was opened September 24, 1994, to investigate relay 162-HVZBB following observation of a dim white control power light. This MWR was voided the same day by the Nuclear Shift Supervisor who was subsequently able to auto start both trains of fans by first placing the control switch in "pull to lock." The shift supervisor attributed this condition to "system design, not equipment deficiency." However, no additional follow-up action was pursued.

To eliminate the sneak circuit path, Design Change 2124 has been implemented to install a blocking diode which will allow relays 162-HVZAB/BB to drop out as required with the fans in standby. The licensee's troubleshooting, as-found testing, design change implementation, and post-modification testing during this inspection period were considered by the inspectors to be thorough and adequate to preclude future auto-start circuitry problems.

3.2. Surveillance Observations

The inspectors witnessed/reviewed selected surveillance tests to determine whether properly approved procedures were in use, details were adequate, test instrumentation was properly calibrated and used, technical specifications were satisfied, testing was performed by qualified personnel, and test results satisfied acceptance criteria or were properly dispositioned. The operational surveillance tests (OSTs), loop calibration procedures (LCPs), and relay calibration procedures (RCPs) listed below were observed and reviewed. Unless otherwise indicated, the activities observed and reviewed were properly conducted without any notable deficiencies.

OST 1.43.6	Containment High Range Monitors Functional Test
OST 1.43.7	Noble Gas Monitor Functional Test
OST 2.47.1	Containment Airlock Test
LCP-2-44F-P21B	Emergency Switchgear Area Supply Pressure Loop Calibration
1/2RCP-30A-PC	Calibration of ATC and Agastat Timing Relays

3.2.1 Supplemental Leak Collection System (SLCRS) Duct Damage at Unit 1

On October 16, 1994, the licensee's Operations Department identified some large holes (several square feet in area) in the SLCRS duct leading to the Unit 1 waste gas storage vault. The licensee also recognized that the deficiency had an outstanding maintenance work request (MWR) that was written in October of 1991. The function of this part of the SLCRS is to maintain a negative pressure on the waste gas storage vault, in order to reduce the magnitude of a radioactive release from a leak in one of the waste gas storage tanks. Any release from the waste gas storage tanks would also be changed to an elevated (vice a ground) release because of the SLCRS. The inspectors reviewed this issue to determine why the licensee had not repaired the damaged duct after almost 3 years, and to evaluate the impact of the damaged duct on the performance of the SLCRS.

The original MWR was categorized as a Priority 2 (urgent/highly desirable), but was downgraded the day after it was written to a Priority 3 (expedite/desirable). The deficiency was not repaired immediately because proper work instructions were not readily available for the repair. Construction maintenance personnel informally told the Engineering Department that they needed a Plant Installation Process Standard (PIPS) to repair the duct. The need for the PIPS was never formally communicated to engineering management personnel, and, thus, a high priority was never given to completing this document. The SLCRS System Engineer was aware of the deficiency, and had adequate test data to demonstrate that SLCRS would perform its design basis functions even with the hole. The test data also showed that the condition was not degrading. Because of the test data, the maintenance engineering and planning personnel did not place a high priority on the repair, and did not

The inspectors observed selected parts of the relay calibrations and the post-maintenance test. The maintenance and testing was adequately controlled. However, the licensee was not using calibrated instrumentation to verify the relay set points during the post-maintenance test. The post-maintenance test procedure specified using the diesel skid-mounted tachometer which is not in the licensee's calibration program. This was pointed out by the inspectors, and the licensee obtained a calibrated stroboscope to ensure the set-points were accurate.
Because of the problems with the No. 1-2 EDG, the licensee checked the operation of the No. 1-1 EDG speed sensing relays during its next regularly scheduled surveillance test. All of the 140 and 870 rpm relays were found slightly out of tolerance, and were adjusted prior to returning the unit to service. The licensee has determined that the repeatability problems with the relays on the No. 1-2 EDG were due to contact corrosion. Other licensee's with the same type of EDGs were contacted, and reported similar problems with the diesel speed sensing circuits. The speed circuit vendor (MKS Power Systems) does not sell a safety-related version of the circuit any more because of the lack of long-term relay reliability. The licensee is going to monitor the performance of the relays during every EDG surveillance test until the next refueling outage. During the refueling outage, the licensee plans to replace the speed sensing circuits with newer, more reliable circuits (similar to the circuits installed at Unit 2).

The inspectors concluded that the licensee's corrective actions to address the problems with the speed sensing circuits were appropriate. The as-found relay set-points would not have affected the operation of the EDGs under design basis conditions. In general, deviations which would have affected EDG operability would have been noted during surveillance testing. The 870 rpm relay which drifted below 490 rpm was also determined not to affect operability. This relay has a close-permissive function for the EDG output breaker; however, the licensee's test data shows that the diesel will reach rated speed before the generator reaches rated output voltage. Therefore, the voltage permissive would have prevented the EDG output breaker from closing early.

The initial actions to address the jacket water low pressure alarm could have been more aggressive. The deficiency was allowed to exist for 4 days before anyone recognized that it might impair operability of the EDG. The licensee's ARP for low jacket water pressure was a contributing factor to the lack of attention to the alarm. The ARP did not consider problems with the speed sensing circuits as a possible cause, and all the verifications required by the procedure led the operators to conclude that the pressure detector had malfunctioned. This observation was discussed with the Unit 1 Operations Manager. The Operations Manager had already arrived at a similar conclusion and was discussing the event at licensed operator retraining.

4.0 ENGINEERING (71707, 37551, 92903)

4.1 AMSAC Design Omission

At Beaver Valley Units 1 and 2, the Anticipated Transient Without Scram (ATWS)

4.2 Calibration of CREBAPS Pressure Switches (Unresolved Item 50-334/94-17-01) (closed)

During a routine walkdown of the control room emergency bottled air pressurization system (CREBAPS), the inspectors noted that several pressure switches, which protect the system from an over-pressure condition, had not been calibrated since 1987. The switches sense a high pressure condition in the piping downstream of the pressure regulators. The licensee initiated calibration checks and an analysis of the failure modes of these switches. The issue was identified as an unresolved item (50-334/94-17-01) pending review of the licensee's failure analysis and the calibration data.

The calibration checks showed that all of the switches would have operated as intended. The licensee's failure modes analysis showed that failure to isolate one of the air lines on a high pressure condition would not challenge the CREBAPS or the control room pressure boundary. However, the licensee found, through recent operating experience, that if a switch fails low, CREBAPS system operation can be degraded (the associated discharge line is disabled). Consequently, the switches will be entered into the licensee's safety-related component calibration program. This issue is closed.

4.3 Solid State Protection System 10 CFR Part 21 (closed)

On September 1, 1994, the Duquesne Light Company submitted a 10 CFR Part 21 report to the NRC concerning the Beaver Valley Unit 1 Solid State Protection System (SSPS). The report concerned an anomaly with the train `B' SSPS semi-automatic tester. The semi-automatic tester is used to test various logic card circuits. The licensee found that the tester card was producing extra test pulses. The extra pulses could prevent testing some logic combinations, which could mask a logic card failure. This problem was discovered by the licensee during troubleshooting of an unrelated logic card failure indication. An observant engineer noticed that the test pulse train on the input of the logic card (with the unrelated failure indication) was not correct.

The licensee found that the system clock counter for the semi-automatic tester was causing the additional pulses. This card was replaced and train `B' of the SSPS was successfully tested. The Unit 1 train `A' and the Unit 2 SSPS logic testers were also checked for proper operation, and no further problems were noted. The licensee has initiated periodic surveillance checks to verify proper operation of all SSPS logic test circuits. Westinghouse has issued a Nuclear Safety Advisory Letter as a result of the Duquesne Light Company findings. The letter recommends that all utilities with Westinghouse solid state protection systems check the semi-automatic test circuits, as a minimum, during each refueling outage.

The inspectors concluded that the licensee demonstrated a strong questioning attitude in the identification of the SSPS semi-automatic tester anomaly, and took appropriate, conservative actions to report and correct the deficiency. This 10 CFR Part 21 issue is considered closed for Beaver Valley.

basis. Licensee personnel were observed to be properly implementing the radiological protection program.

5.2 Security

Implementation of the physical security plan was observed in various plant areas with regard to the following: protected area and vital area barriers were well maintained and not compromised; isolation zones were clear; personnel and vehicles entering and packages being delivered to the protected area were properly searched and access control was in accordance with approved licensee procedures; persons granted access to the site were badged to indicate whether they have unescorted access or escorted authorization; security access controls to vital areas were maintained and persons in vital areas were authorized; security posts were adequately staffed and equipped, security personnel were alert and knowledgeable regarding position requirements, and that written procedures were available; and adequate illumination was maintained. Licensee personnel were observed to be properly implementing and following the Physical Security Plan.

5.3 Housekeeping

Plant housekeeping controls were monitored, including control and storage of flammable material and other potential safety hazards. The inspectors conducted detailed walkdowns of accessible areas of both Unit 1 and Unit 2. There has been improvement in housekeeping since the last inspection period, and the inspectors have noted management attention to housekeeping.

6.0 ADMINISTRATIVE

6.1 Preliminary Inspection Findings Exit

At periodic intervals during this inspection, meetings were held with senior plant management to discuss licensee activities and inspector areas of concern. Following conclusion of the report period, the resident inspector staff conducted an exit meeting on November 16, 1994, with Beaver Valley management summarizing inspection activity and findings for this period.

6.2 Attendance at Exit Meetings Conducted by Region-Based Inspectors

During this inspection period, the inspectors attended the following exit meetings:

Dates	Subject	Inspection Report No.	Reporting Inspector
October 14, 1994	Engineering	94-22/23	R. Paolino
October 14, 1994	Unit 1 SRO Exams	94-21	P. Bissett
October 28, 1994	EDSFI Open Items	94-25/26	R. Bhatia
November 10, 1994	MOV Open Items	94-23/24	F. Bower

Table of Contents

List of Tables

4.12 Emergency Action Levels

4.12.1 Learning Objectives

1. State the purpose of the Emergency Action Levels.
2. List the four Emergency Classification Levels in order of severity.
3. List the four documents used to establish Emergency Action Levels.

4.12.2 Introduction

The purpose of an Emergency Action Level (EAL) is to trigger the declaration of an emergency classification level (ECL), which, in turn, triggers a certain level of emergency response. These actions are directed toward providing information to offsite emergency response authorities and federal agencies (e.g. plant conditions, meteorological conditions, radiological field monitoring results). Licensees' actions to respond directly to the onsite situation are governed by emergency operating procedures. Emergency action levels are used by plant personnel in determining the appropriate ECL to declare.

In paragraph 50.47, "Emergency Plans," of 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," paragraph (a)(1) states that no operating license for a nuclear power reactor will be issued unless a finding is made by the NRC that there is reasonable assurance that adequate protective measures can and will be taken in the event of a radiological emergency. For operating power reactors, 10 CFR 50.54(s)(2)(ii) requires that "If... the NRC finds that the state of emergency preparedness does not provide reasonable assurance that adequate protective measures can and will be taken in the event of a radiological emergency... the Commission will determine whether the reactor shall be shutdown until such deficiencies are remedied.

Onsite and Offsite emergency response plans must meet the standards that are listed in 10 CFR 50.47 in order for the staff to make a positive finding that there is reasonable assurance that adequate protective measures can and will be taken in the event of a radiological emergency. One of these standards, 10 CFR 50.47(b)(4), pertains to the development of emergency classification and actions level scheme. Section IV", Content of Emergency Plans", of Appendix E to 10 CFR Part 50 also contains requirements for the development and review of EALs.

Revision 1 to NUREG-0654/FEMA-REP-1, "Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants," was published in November 1980 to provide specific acceptance criteria for complying with the standards set forth in 10 CFR 50.47.

In January 1992, the Nuclear Utilities Management and Resource Council (NUMARC) issued Revision 2 of NUMARC/NESP-007, "Methodology for Development for Emergency Action Levels", which contained guidance on EAL development that accounted for lessons learned from the ten years of using the NUREG-0654 guidance. The NRC stated in Revision 3 of Regulatory Guide 1.101, that revision 2 of NUMARC/NESP-007 was considered to be an acceptable alternative to the guidance provided in NUREG-0654 for development of EALs to comply with 10 CFR 50.47 and Appendix E to 10 CFR Part 50. In addition, the need for further guidance for developing emergency action levels applicable in the shutdown and refueling modes of operation were identified in Revision 3 to Regulatory Guide 1.101.

On February 28, 2000, the Nuclear Energy Institute (NEI) submitted NEI 99-01, Methodology for Development of Emergency Action Levels. The NEI 99-01 methodology is very similar to the NUMARC/NESP-007 methodology with guidance provided on initial condition (IC), example EALs and a basis for each IC and EAL. NEI 99-01 incorporated new EAL guidance for (1) Shutdown and refueling modes of plant operation, (2) permanently defueled plants, and (3) Independent Spent Fuel Storage Installations (ISFSIs).

Prior revisions to Revision 4 of Regulatory Guide 1.101 stated that "Licensees may use either NUREG-0654/FEMA-REP-1or NUMARC/NESP-007 in developing their EAL scheme but may not use portions of both methodologies." The staff stated in Emergency Preparedness Position on Acceptable Deviations from Appendix 1 of NUREG-0654 based upon the Staff's regulatory analysis of NUMARC/NESP-007 that it recognizes that licensees who continue to use EALs based upon NUREG-0654 could benefit from the technical basis from EALs provided in NUMARC/NESP-007. However, the staff also recognized that the classification scheme must remain internally consistent. Likewise, Licensees can benefit from guidance provided in NEI 99-01 without revising their entire EAL scheme. This is particularly true in regard to adopting guidance on EALs for cold shutdown and refueling modes of operation or for Independent Fuel Storage facilities. However, the licensee still needs to ensure that its EAL scheme remains internally consistent.

4.12.3 NUREG-0654

NUREG-0654/FEMA-REP-1 was published to provide a common reference and guidance source for:

- Nuclear facility operators as well as State and local governments in the development of radiological emergency response plans and preparedness in support of nuclear power plants.
- Federal Emergency management Agency (FEMA), Nuclear Regulatory Commission (NRC), and other Federal agency personnel engaged in the review of State and, Local government and licensee plans and preparedness.
- FEMA, NRC and other Federal agencies in the development of the National Radiological Emergency Plan.

NUREG-0654/FEMA-REP-1 was prepared as part of their responsibilities under the Atomic Energy Act, as amended, and the President's Statement of December 7, 1979, with the accompanying Fact Sheet. The responsibilities include development and promulgation of guidance to nuclear facility operators, State and local governments, in cooperation with other Federal agencies. The guidance included preparation of radiological emergency response plans and assessing the adequacy of such plans.

4.12.3.1 NUREG-0654/FEMA-REP-1, Appendix- 1

Appendix 1 of NUREG-0654/FEMA-REP-1, contains the Emergency Action Level Guidelines for Nuclear Power Plants. Within Appendix 1 four classes of Emergency Classification Levels (EAL) are established:

- Notification of Unusual Event
- Alert
- Site Area Emergency
- General Emergency

A graduation is provided to assure fuller response preparations for more serious indicators. The rationale for the notification and alert classes is to provide early and prompt notification of minor events which lead to more serious consequences given operator error or equipment failure or which might be indicative of more serious conditions which are not yet realized. The site area emergency class reflects conditions where some significant releases are likely or are occurring but where a core melt situation is not indicated based on current information. In this situation full mobilization of emergency personnel in the near site environs is indicated as well as dispatch of monitoring teams and associated communications. The general emergency class involves actual or imminent substantial core degradation or core melting with potential for loss of containment. The immediate action for this class is sheltering (staying inside) rather than evacuation until assessment can be made that (1) an evacuation is indicated and (2) an evacuation, if indicated, can be completed prior to significant release and transport of radioactive material to the affected areas.

Facility licensees have primary responsibility for accident assessment. This includes prompt action to evaluate any potential risk to the public health and safety, both onsite and offsite, and timely recommendations to State and local governments concerning protective measures. The criteria for identification and classification of accidents and the notification of offsite agencies by the facility licensee are set forth in Appendix 1 of NUREG-0654/FEMA-REP-1 (Tables 4.12-1...4).

Because of the potential need to take immediate action offsite in the event of a significant radiological accident, notifications to appropriate offsite response organizations must come directly from the facility licensee. The response organizations which receive these notifications should have the authority and capability to take immediate predetermined actions based on recommendations from the facility licensee. These actions could include prompt notification of the public in the offsite area, followed by advisories to the public in certain areas to stay inside or, if appropriate, evacuate to predetermined relocation host areas.

The lowest level of emergency action levels, Notification of Unusual Events classification, is comprised of event in progress, or which have occurred, that indicate a potential degradation of the level of safety of the station. These types of events may progress to more severe emergency classification if they are not mitigated. No releases of radioactive material requiring offsite response or monitoring are expected unless further degradation of safety systems occurs. Examples of Notification of Unusual Events and actions for the facility licensee as well as the State and local authorities are listed in Table 4.12-1.

The next classification, Alert, is comprised of events in progress, or which have occurred, that involve actual or potentially substantial degradation of the safety level of the station. At this classification level, minor releases of radioactivity may occur or may have occurred. Any releases expected to be limited to small fractions of EPA Protective Action Guideline exposure levels. Examples of Alert events and actions for the facility licensee as well as the State and local authorities are listed in Table 4.12-2.

The Site Area Emergency classification is the second highest classification. Site Area Emergency is comprised of events in progress, or which have occurred, that involve actual or potential major failure of plant functions needed for protection of the public. Releases are not expected to exceed EPA Protective Action Guidelines, except near the Site Boundary. Examples of Site Area Emergency events and actions for the facility licensee as well as the State and local authorities are listed in Table 4.12-3.

The highest level classification, General Emergency, is comprised of events in progress, or which have occurred, that involve actual or imminent substantial core degradation or melting with a potential for the loss of the primary containment integrity. Release can be reasonably expected to exceed EPA Protective Action Guideline exposure levels offsite for more than the immediate site area. Examples of General Emergencies and actions for the facility licensee as well as the State and local authorities are listed in Table 4.12-4.

4.12.4 NUMARC/NESP-007

The NUMARC/NESP-007 was developed to replace NUREG-0654/FEMA-REP-1. The NUMARC/NESP-007 methodology provides guidance on Initial Conditions (ICs) and example Emergency Action Levels (EALs), for each IC and a basis for IC and EALs. NUMARC/NESP-007 has three types of ICs and EALs:

- Symptom based
- Event based
- Barrier based

The symptom based EALs refer to those indicators that are measurable over a continuous spectrum, (e.g. core temperature, coolant level, radiation meter readings). Off-normal readings on such indicators are symptoms of problems. The seriousness of a symptom depends on such factors as the degree to which technical specifications are exceeded and the capability of licensed operators to gain control and bring the indicators back to safe levels. Event-based ICs and EALs refer to discrete occurrences with potential safety significance such as a fire or severe weather. Barrier-based ICs and EALs utilize indications of the level of challenge to the principal barriers used to assure containment of radioactive materials within a nuclear plant. For the most important type of radioactive material, i.e., fission products, there are three principal barriers:

- Fuel cladding
- Reactor coolant system boundary
- Containment

In the NUMARC/NESP-007 methodology, the operating modes (power operation, startup, hot standby, hot shutdown, cold shutdown, refueling, and defueled) to which individual ICs apply are specified. As a plant moves from power operation through the decay heat removal process toward cold shutdown and refueling, barriers to the release of fission products may be reduced, instrumentation to detect symptoms may not be fully effective and partially disabling of safety systems may be permitted by technical specifications. For such operations, ICs and EALs tend to be event-based rather than symptom-based.

The ICs and EALs are divided into four "recognition categories" in NUMARC/NESP-007:

- A - Abnormal Rad Levels/Radiological Effluent
- F - Fission Product Barrier Degradation
- H - Hazards or Other Conditions Affecting Plant Safety
- S - System Malfunction

For recognition categories A, H, and S, ICs and associated EALs are developed for each emergency classification level. For these recognition categories, ICs are identified by a three character acronym. For example, AU2 is the second Unusual Event IC in the Abnormal Radiation Level recognition category and SS3 is the third Site Area Emergency IC in the System Malfunction recognition category.

For recognition category F, there are three ICs:

1. Loss or potential loss of the fuel clad barrier, and
2. Loss or potential loss of the RCS barrier.
3. Loss or potential loss of the containment barrier.

The EALs for each of these ICs depend on whether the reactor is a PWR or BWR. The emergency condition level is a function of the number (and extent) of fission product barrier degradation, as indicated below:

UNUSUAL EVENT	Any loss or potential loss of containment
ALERT	Any loss or any potential loss of either fuel clad or RCS
SITE AREA EMERGENCY	Loss of both fuel clad and RCS; or Potential loss of either; or Potential loss of either, and loss of any additional barrier
GENERAL EMERGENCY	Loss of two barriers and potential loss of the third barrier

Table 4.12-6 provides an example of an emergency action level (EBD-S) bases document for system malfunction category SU5. The acronym SU5 is the fifth Unusual Event IC in the System Malfunction recognition category.

4.12.5 NEI 99-01 (NUMARC/NESP-007- Rev. 4)

Revision 4 to NUMARC/NESP-007 (NEI 99-01) presents the methodology for development of emergency action levels as an alternative to NRC/FEMA guidelines contained in Appendix 1 of NUREG-0654/FEMA-REP-1, Rev.2 "Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of nuclear Power Plants," October 1980 and 10 CFR 50.47 (a)(4). Revision 4 of NUMARC/NESP-007 enhances Revision 3 (NEI 97-03) by considering the system malfunction initiating conditions and example emergency action levels which address conditions that maybe postulated to occur at nuclear power plants during plant shutdown conditions. Also included are initiating conditions and example emergency action levels that fully address conditions that may be postulated to occur at permanently Defueled Stations and Independent Spent Fuel Storage Installations.

4.12.6 Regulatory Guide 1.101

Regulatory guides are issued to describe and make available to the public such information as methods acceptable to the NRC staff for implementing specific parts of the NRC's regulations, techniques used by staff in evaluating specific problems or postulated accidents, and data needed by the NRC staff in its review of applications for permits and licenses. Regulatory guides are not substitutes for regulations, and compliance with them is not required. Methods and solutions different from those set out in the guides will be acceptable if they provide a basis for the findings requisite to the issuance or continuance of a permit or license by the commission.

Prior revisions to Regulatory Guide 1.101 (revisions 1, 2, and 3) stated that "Licensees may use either NUREG-0654/FEMA-REP-1or NUMARC/NESP-007 in developing their EAL scheme but may not use portions of both methodologies." The staff stated in, Emergency Preparedness Position on Acceptable Deviations from Appendix 1 of NUREG-0654 based upon the Staff's regulatory analysis of NUMARC/NESP-007 that it recognizes that licensees who continue to use EALs based upon NUREG-0654 could benefit from the technical basis from EALs provided in NUMARC/NESP-007. However, the staff also recognized that the classification scheme must remain internally consistent.

The Staff is proposing a revision to Regulatory Guide1.101 which will endorse NEI 99-01. Licensees would be able to benefit from guidance provided in NEI 99-01 without revising their entire EAL scheme. This is particularly so in regards to adopting guidance on EALs for cold shutdown and refueling modes of operation or for Independent Fuel Storage facilities. However, the licensee needs to ensure that its EAL scheme remains internally consistent.

4.12.7 Summary

The NRC decision process for determining the nature of and level of effort for NRC responses to reactor events or conditions that could affect the health and safety of the public must include all available information and insights regarding the affected reactor plant. The numerical risk estimation guidelines are not meaningful unless they are accompanied by an understanding of the most influential assumptions and uncertainties that stand behind them. It is the understanding (not the numerical result alone) that is intended to aid NRC inspectors and management in assessing the potential degree of loss of defense-in-depth as a input to determining the appropriate NRC response to events.

The purpose of an Emergency Action Level (EAL) is to trigger the declaration of an emergency classification level (ECL), which, in turn, triggers a certain level of emergency response. These actions are directed toward providing information to offsite emergency response authorities and federal agencies (e.g. plant conditions, meteorological conditions, radiological field monitoring results). Licensees' actions to respond directly to the onsite situation are governed by emergency operating procedures. Emergency action levels are used by plant personnel in determining the appropriate ECL to declare. Nuclear Power Plants write their procedures by following at least one of the three emergency response plans:

- Revision 1 to NUREG-0654/FEMA-REP-1, "Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants,"
- Nuclear Utilities Management and Resource Council (NUMARC) issued Revision 2 of NUMARC / NESP-007, "Methodology for

Development for Emergency Action Levels"

- Nuclear Energy Institute (NEI) submitted NEI 99-01, Methodology for Development of Emergency Action Levels

Onsite and Offsite emergency response plans must meet the standards that are listed in 10 CFR 50.47 in order for the staff to make a positive finding that there is reasonable assurance that adequate protective measures can and will be taken in the event of a radiological emergency. One of these standards, 10 CFR 50.47(b)(4), pertains to the development of emergency classification and actions level scheme. Section IV", Content of Emergency Plans", of Appendix E to 10 CFR Part 50 also contains requirements for the development and review of EALs.

Table 4.12-1 NUREG 0654/FENA-REP-1 (NUE)

Class	**Licensee Actions**	**State and/or Local Offsite Authority Actions**
Notification of Unusual Event	1. Promptly inform State and/or local offsite authorities of nature of unusual condition as soon as discovered	1. Provide fire or security assistance if requested
Class Description	2. Augment on-shift resources as needed	2. Escalate to a more severe class, if appropriate
	3. Assess and respond	3. Stand by until verbal closeout
Unusual events are in progress or have occurred which indicate a potential degradation of the level of safety of the plant. No releases of radioactive material requiring offsite response or monitoring are expected unless further degradation of safety systems occur	4. Escalate to a more severe class, appropriate or 5. Close out with verbal summary to offsite authorities; followed by written summary within24 hours	
Purpose		
1. Assure that the first step in any response later found to be necessary has been carried out.		
2. Bring the operating staff to a state of readiness.		
3. Provide systematic handling of unusual events information and decision making.		

Table 4.12-1 EXAMPLE INITIATING CONDITIONS: NUE

1. Emergency Core Cooling System (ECCS) initiated and discharge to vessel

2. Radiological effluent technical specification limits exceeded

3. Fuel damage indication. Examples·
   a. High offgas at BWR air ejector monitor (greater than 500,000 uci/sec; corresponding to 16 isotopes decayed to 30 minutes; or an increase of 100,000 uci/sec within a 30 minute time period)
   b. High coolant activity sample (e.g., exceeding coolant technical specifications for iodine spike)

4. Abnormal coolant temperature and/or pressure or abnormal fuel temperatures outside of technical specification limits

5. Exceeding either primary/secondary leak rate technical specification or primary system leak rate technical specification

6. Failure of a safety or relief valve in a safety related system to close following reduction of applicable pressure

7. Loss of offsite power or loss of onsite AC power capability

8. Loss of containment integrity requiring shutdown by technical specifications

9. Loss of engineered safety feature or fire protection system function requiring shutdown by technical specifications (e.g., because of malfunction, personnel error or procedural inadequacy)

10. Fire within the plant lasting more than 10 minutes

11. Indications or alarms on process or effluent parameters not functional in control room to an extent requiring plant shutdown or other significant loss of assessment or communication capability (e.g., plant computer, Safety Parameter Display System, all meteorological instrumentation)

12. Security threat or attempted entry or attempted sabotage

13. Natural phenomenon being experienced or projected beyond usual levels
    a. Any earthquake felt in-plant or detected on station seismic instrumentation
    b. 50 year flood or low water, tsunami, hurricane surge
    c. Any tornado on site
    d. Any hurricane

14. Other plant conditions exist that warrant increased awareness on the part of a plant operating staff or State and/or local offsite authorities or require plant shutdown under technical specification requirements or involve other than normal controlled shutdown (e.g., cooldown rate exceeding technical specification limits, pipe cracking found during operation)

15. Transportation of contaminated injured individual from site to offsite hospital

Table 4.12-2 NUREG 0654/FENA-REP-1 (Alert)

Class

ALERT

Class Description

Events are in progress or have occurred which involve an actual or potential substantial degradation of the level of safety of the plant. Any releases expected to be limited to small fractions of the EPA Protective Action Guideline exposure levels.

Purpose

1. Assure that emergency personnel are readily available to respond if situation becomes more serious or to perform confirmatory radiation monitoring if required
2. Provide offsite authorities current status information

Licensee Actions

1. Promptly inform State and/or local authorities of alert status and reason for alert as soon as discovered
2. Augment resources and activate on-site Technical Support Center and on-site operational support center. Bring Emergency Operations Facility (EOF) and other key emergency personnel to standby status
3. Assess and respond
4. Dispatch on-site monitoring teams and associated communications
5. Provide periodic plant status updates to offsite authorities (at least every 15 minutes)
6. Provide Periodic meteorological assessments to offsite authorities and, if any releases are occurring , dose estimates for actual releases.
7. Escalate to a more severe class, if appropriate
8. Close out or recommend reduction in emergency class by verbal summary to offsite authorities followed by written summary within 8 hours of closeout or class reduction.

State and/or Local Offsite Authority Actions

1. Provide fire or security assistance if requested
2. Augment resources and bring primary response centers and EBS to standby status
3. Alert to standby status key emergency personnel including monitoring teams and associated communications
4. Provide confirmatory offsite radiation monitoring and ingestion pathway dose projections if actual releases substantially exceed technical specification limits
5. Escalate to a more severe class, if appropriate
6. Maintain alert status until verbal closeout or reduction of emergency class

Table 4.12-2 EXAMPLE INITIATING CONDITIONS: ALERT

1. Severe loss of fuel cladding
   a. High offgas at BWR air ejector monitor (greater than 5 ci/sec; corresponding to 16 isotopes decayed 30 minutes)
   b. Very high coolant activity sample (e.g., 300 uci/cc equivalent of 1-131)
   c. Failed fuel monitor (PWR) indicates increase greater than 1% fuel failures within 30 minutes or 5% total fuel failures.

2. Severe Natural phenomena being experienced or projected
   a. Earthquake greater than OBE levels
   b. Flood
   c. Any tornado striking the facility

3. Steam line break with significant (e.g., greater than 10 gpm) primary to secondary leak rate (PWR) or MSIV malfunction causing leakage (BWR)

4. Primary coolant leak rate greater than 50 gpm

5. Radiation levels or airborne contamination which indicate a severe degradation in the control of radioactive materials (e.g., increase of factor of 1000 in direct radiation readings within facility)

6. Loss of offsite power and loss of all onsite AC power (see Site Area Emergency for extended loss)

7. Loss of all onsite DC power (See Site Area Emergency for extended loss)

8. Coolant pump seizure leading to fuel failure

9. Complete loss of any function needed, for plant cold shutdown

10. Failure of the reactor protection system to initiate and complete a scram which brings the reactor subcritical

11. Fuel damage accident with release of radioactivity to containment or fuel handling building

12. Fire potentially affecting safety systems

13. Most or all alarms (annunciators) lost

14. Radiological effluents greater than 10 times technical specification instantaneous limits (an instantaneous rate which, if continued over 2 hours, would result in about 1 mr at the site boundary under average meteorological conditions)

15. Ongoing security compromise

16. Other plant conditions exist that warrant precautionary activation of technical support center and placing near-site Emergency Operations Facility and other key emergency personnel on standby

17. Evacuation of control room anticipated or required with control of shutdown systems established from local stations

Table 4.12-3 NUREG 0654/FENA-REP-1 (SAE)

Class

Site Area Emergency

Class Description

Events are in process or have occurred which involve actual or likely major failures of plant functions needed for protection of the public. Any releases not expected to exceed EPA Protective Action Guideline exposure levels except near site boundary.

Purpose

1. Assure that response centers are manned.
2. Assure that monitoring teams are dispatched
3. Assure that personnel required for evacuation of near-site areas are at duty stations if situations becomes more serious
4. Provide consultation with offsite authorities
5. Provide updates for the public through offsite authorities.

Licensee Actions

1. Promptly inform State and/or local offsite authorities of site area emergency status and reason for emergency as soon as discovered.
2. Augment resources by activating on-site Technical Support Center, on-site operational support center and near-site Emergency Operations Facility (EOF)
3. Assess and respond.
4. Dispatch on-site and offsite monitoring teams and associated communications
5. Dedicate an individual for plant status updates to offsite authorities and periodic press briefing(perhaps joint with offsite authorities)
6. Make senior technical and management staff onsite available for consultation with NRC and State on a periodic basis.
7. Provide meteorological and dose estimates to offsite authorities for actual releases via a dedicated individual or automated data transmission.
8. Provide release and dose projections based on available plant condition information and foreseeable contingencies.
9. Escalate to General Emergency class, if appropriate

or

10. Close out or recommend reduction in emergency class by briefing of offsite authorities at EOF and by phone followed by written summary within 8 hours of closeout or class reduction

State and/or Local Offsite Authority Actions

1. Provide any assistance requested.
2. If sheltering near the site is desirable, activate public notification system within at least two miles of the plant.
3. Provide public within at least about 10 miles periodic updates on emergency status.
4. Augment resources by activating primary response centers.
5. Dispatch key emergency personnel including monitoring teams and associated communications.
6. Alert to standby status other emergency personnel (e.g. those needed for evacuation) and dispatch personnel to near-site duty stations.
7. Provide offsite monitoring results to licensee, DOE and others and jointly assess them.
8. Continuously assess information from licensee and offsite monitoring with regard to changes to protective actions already initiated for public and mobilizing evacuation resources.
9. Recommend placing milk animals within 2 miles on stored feed and assess need to extend distance.
10. Provide press briefings, perhaps with licensee.
11. Escalate to General Emergency class, if appropriate.
12. Maintain site area emergency status until closeout or reduction of emergency class.

Table 4.12-3 EXAMPLE INITIATING CONDITIONS: SAE

1. Known loss of coolant accident greater than makeup pump capacity

2. Degraded core with possible loss of coolable geometry (indicators should include instrumentation to detect inadequate core cooling, coolant activity and/or containment radioactivity levels)

3. Rapid failure of steam generator tubes (several hundred gpm leakage) with loss of offsite power

4. BWR steam line break outside containment without isolation

5. Loss of offsite power and loss of onsite AC power for mote than 15 minutes

6. Loss of all vital onsite DC power for more than 15 minutes

7. Complete loss of any function needed for plant hot shutdown

8. Transient requiring operation of shutdown systems with failure to scram (continued power generation but no core damage immediately evident)

9. Major damage to spent fuel in containment or fuel handling building (e.g., large object damages fuel or water loss below fuel level)

10. Fire compromising the functions of safety systems

12. Most or all alarms (annunciators) lost and plant transient initiated or in progress

13. a. Effluent monitors detect levels corresponding to greater than 50 mr/hr for 112 hour or greater than 500 mr/hr W.B. for two minutes (or five times these levels to the thyroid) at the site boundary for adverse meteorology
    b. These dose rates are projected based on other plant parameters (e.g., radiation level in containment with leak rate appropriate for existing containment pressure) or are measured in the environs
    c. EPA Protective Action Guidelines are projected to be exceeded outside the site boundary

14. Imminent loss of physical control of the plant

15. Severe natural phenomena being experienced or projected with plant not in cold shutdown
    a. Earthquake greater than SSE levels
    b. Flood, low water, tsunami, hurricane greater than design levels or failures of protection of vital equipment at lower levels
    c. Sustained winds or tornadoes in excess of design levels.

16. Other plant conditions exist that warrant activation of emergency centers and monitoring teams or a precautionary notification to the public near the site.

17. Evacuation of control room and control of shutdown systems not established from local stations in 15 minutes.

Table 4.12-4 NUREG 0654/FENA-REP-1 (GE)

Class	Licensee Actions	State and/or Local Offsite Authority Actions
General Emergency **Class Description** Events are in process or have occurred which involve actual or imminent substantial core degradation or melting with potential for loss of containment integrity. Releases can be reasonably expected to exceed EPA Protective Action Guideline exposure levels offsite for more that the immediate site area. **Purpose** 1. Initiate predetermined protective actions for the public. 2. Provide continuous assessment of information from licensee and offsite organization measurements. 3. Initiate additional measures as indicated by actual or potential releases. 4. Provide consultation with offsite authorities. 5. Provide updates for the public through offsite authorities.	1. Promptly inform State and local offsite authorities of general emergency status and reason for emergency as soon as discovered (Parallel notification of State/local). 2. Augment resources by activating on-site Technical Support Center, on-site operational support center and near-site Emergency Operations Facility (EOF). 3. Assess and respond. 4. Dispatch on-site and offsite monitoring teams and associated communications. 5. Dedicate an individual for plant status updates to offsite authorities and periodic press briefing (perhaps joint with offsite authorities). 6. Make senior technical and management staff onsite available for consultation with NRC and State on a periodic basis. 7. Provide meteorological and dose estimates to offsite authorities for actual releases via a dedicated individual or automated data transmission. 8. Provide release and dose projections based on available plant condition information and foreseeable contingencies. 9. Close out or recommend reduction in emergency class by briefing of offsite authorities at EOF and by phone followed by written summary within 8 hours of close out or class reduction.	1. Provide any assistance requested. 2. Activate immediate public notification of emergency status and provide public periodic updates. 3. Recommend sheltering for 2 mile radius and 5 miles downwind and assess need to extend distances. Consider advisability of evacuation. (projected time available vs. estimated evacuation times) 4. Augment resources by activating primary response centers. 5. Dispatch key emergency personnel including monitoring teams and associated communications. 6. Dispatch other emergency personnel to duty stations within 5 mile radius and alert all others to standby status. 7. Provide offsite monitoring results to licensee, DOE and others and jointly assess them. 8. Continuously assess information from licensee and offsite monitoring with regard to changes to protective actions already initiated for public and mobilizing evacuation resources. 9. Recommend placing milk animals within 10 miles on stored feed and assess need to extend distance. 10. Provide press briefings, perhaps with licensee. 11. Maintain general emergency status until closeout or reduction of emergency class.

Table 4.12-4 EXAMPLE INITIATING CONDITIONS: GE

1. a. Effluent monitors detect levels corresponding to 1, rem/hr W.B. or 5 rem/hr thyroid at the site boundary under actual.,meteorological conditions
   b. These dose rates are projected based on other plant parameters (e.g., radiation levels in containment with leak rate appropriate for existing containment pressure with some confi mation from effluent monitors) or are measured in the environs

Note: Consider evacuation only within about 2 miles of the site boundary unless these site boundary levels are exceeded by a factor of 10 or projected to continue for 10 hours or EPA Protective Action Guidelne exposure levels are predicted to be exceeded at longer distances

2. Loss of 2 of 3 fission product barriers with a potential loss of 3rd barrier, (e.g., loss of primary coolant boundary, clad failure, and high potential for loss of containment)

3. Loss of physical control of the facility

Note: Consider 2 mile precautionary evacuation

4. Other plant conditions exist, from whatever source, that make release of large amounts of radioactivity in a short time period possible, e.g., any core melt situation. See the specific PWR and BWR sequences below.

Notes:
a. For core melt sequences where significant releases from containment are not yet taking place and large amounts of fission products are not yet in the containment atmosphere, consider 2 mile precautionary evacuation. Consider 5 mile, downwind evacuation (450 to 900 sector) if large amounts of fission products (greater than gap activity) are in the containment atmosphere. Recommend sheltering in other parts of the plume exposure Emergency Planning Zone under this circumstance.
b. For core melt sequences where significant releases from containment are not yet taking place and containmentlailure leading to a direct atmospheric release is likely in the sequence but not imminent and large amounts of fission products in addition to noble gases are in the containment atmosphere, consider precautionary evacuation to 5 miles and 10 mile downwind evacuation (450 to 900 sector).
c. For core melt sequences where large amounts'of fission products other than noble gases are in the containment atmosphere and containment failure is judged imminent, recommend shelter for those areas where evacuation cannot be completed before transport of activity to that location.
d. As release information becomes available adjust these actions in accordance with dose projections, time available to evacuate and estimated evacuation times given current conditions.

6. Example BWR Sequences
   a. Transient (e.g., loss of offsite power) plus failure of requisite core shut down systems (e.g., scram). Could lead to core melt in several hours with containment failure likely. More severe consequences if pumps trip does not function.
   b. Small or large LOCA's with failure of ECCS to perform leading to core melt degradation or melt in minutes to hours. Loss of containment integrity may be imminent.
   c. Small or large LOCA occurs and containment performance is unsuccessful affecting longer term success of the ECCS. Could lead to core degradation or melt in several hours without containment boundary.
   d. Shutdown occurs but requisite decay heat removal systems (e.g., RHR) or non-safety systems heat removal means are rendered unavailable. Core degradation or melt could occur in about ten hours with subsequent containment failure.

Table 4.12-5 NUMARC/NESP-007
Recognition Category S
System Malfunction
Initiating Condition Matrix

NOUE		ALERT		SITE AREA EMERGENCY		GENERAL EMERGENCY	
SU1	Loss of All Offsite Power to Essential Busses for Greater Than 15 Minutes. Modes: PO,SU,Hstby, Hsd	SA1	AC power capability to essential busses reduced to a single power source for greater than 15 minutes such that any additional single failure would result in station blackout. Modes: PO,SU,Hstby, Hsd	SS1	Loss of All Offsite Power and Loss of All Onsite AC Power to Essential Busses. Modes: PO,SU,Hstby, Hsd	SG1	Prolonged Loss of Offsite Power and Prolonged Loss of All Onsite AC Power to essential Busses. Modes: PO,SU,Hstby, Hsd
SU2	Inability to reach required shutdown within technical specification limits.. Modes: PO,SU,Hstby, Hsd	SA2	Failure of reactor protection instrumentation to complete or initiate an automatic reactor scram once a reactor protection system setpoint has been exceeded and manual scram was successful. Modes: PO,SU,Hstby	SS2	Failure of reactor protection instrumentation to complete or initiate an automatic reactor scram once a reactor protection system setpoint has been exceeded and manual scram was NOT successful. Modes: PO,SU	SG2	Failure of reactor protection instrumentation to complete an automatic reactor scram and manual scram was NOT successful and there is indication of an extreme challenge to the ability to cool the core. Modes: PO,SU
SU3	UNPLANNED loss of most or all safety system annunciation or indication in the control room for greater than 15 minutes. Modes: PO,SU,Hstby,Hsd	SA3	UNPLANNED loss of most or all safety system annunciation or indication in the control room with either (1) a SIGNIFICANT TRANSIENT in progress, or (2) Compensatory non-alarming indicators are unavailable.	SS3	Inability to monitor a SIGNIFICANT TRANSIENT in Progress.	SG3	
SU4	Fuel clad degradation. Modes: PO,SU,Hstby,Hsd	SA4		SS4		SG4	
SU5	RCS leakage. Modes: PO,SU,Hstby, Hsd	SA5		SS5		SG5	
SU6	UNPLANNED Loss of all onsite or offsite communications capabilities. Modes: PO,SU,Hstby, Hsd	SA6		SS6		SG6	
SU7	Inadvertent Criticality. Modes: Hstby, Hsd	SA7		SS7		SG7	

Table 4.12-6 EAL BASES DOCUMENT (EBD-S)

EAL BASES DOCUMENT (EBD-S)
SYSTEMS MALFUNCTION CATEGORY

SU5 RCS Leakage

EVENT TYPE: Coolant Leak

OPERATING MODE APPLICABILITY: Run, Startup, Hot Shutdown

THRESHOLD VALUE: One of the following:

I. Unidentified or pressure boundary leakage greater than 10 gpm. **OR**

2. Identified leakage greater than 25 gpm. **OR**

3. Valid indication of Main Steamline Break.

SHOREHAM EAL INFORMATION:

EAL Threshold Values 1 and 2 are precursors of more serious RCS barrier challenges and are thus considered as a potential degradation of the level of safety of the plant. Thus, it is possible to be operating within Technical Specification LCO Action Statement time limits and make a declaration of an Unusual Event in accordance with these EALs. Credit for the action statement time limit should only be given when leakage exceeds technical specification limits but has not yet exceeded the Unusual Event EAL thresholds described above. In addition, indication of main steam line break has been added here as discussed in *NUMAR C Methodology for Development of Emergency Action Levels NUMARCINESP-007 Revision 2 Questions and Answers*, June 1993, Fission Product Barrier-BWR section. This was in response to question 4 which states that the main steam line break with isolation can be classified under System Malfunctions.

Valid means that the reading is from instrumentation determined to be operable in accordance with the Technical Specifications or has been verified by other independent methods such as indications displayed on the control panels, reports from plant personnel, or radiological survey results.

Tech Spec Section 3.4.4 coolant system leakage LCO limits are: (1) :no pressure boundary leakage, (2) :@ 5 gpm unidentified leakage, (3) :@ 25 gpm total leakage averaged over the previous 24 hour period, and (4) @ 2 gpm increase in unidentified leakage within the previous 24 hour period in Mode 1. Total leakage is defined as the sum of identified and unidentified leakage.

Table 4.12-6 EAL BASES DOCUMENT (EBD-S)

EAL BASES DOCUMENT (EBD-S)
SYSTEMS MALFUNCTION CATEGORY

The EAL Threshold Value 1 uses the generic value of 10 GPM for unidentified leakage or pressure boundary leakage. The 10 gpm value for the unidentified or pressure boundary leakage was selected as it is observable with normal control room indications. Threshold Value 2 uses identified leakage set at a higher value due to the lesser significance of identified leakage in comparison to unidentified or pressure boundary leakage.

REFERENCES:

1 .Technical Specification 3.4.4, Coolant Leakage

2. Surveillance Test Procedure No. (STP) 3.0.0.0-01, Reactor Coolant System Leak Rate Calculation

3. Operating Instruction No. (01) 920, Drywell Sump System

4. Alarm Response Procedure (ARP) I C04B, Reactor Water Cleanup and Recirculation

5. Alarm Response Procedure (ARP) I C04C, Reactor Water Cleanup and Recirculation

6. UFSAR Section 5.2.5, Detection of Leakage through Reactor Coolant Pressure Boundary

7. UFSAR Section 15.6.6, Loss-of-Coolant-Accident

8. *NEI Methodology for Development of Emergency Action Levels NUMARCINESP-007 Revision* 4, May 1999

Boiling Water Reactor
GE BWR/4
Technology Advanced Manual

Chapter 5.0

<u>Transients</u>

Table of Contents

List of Tables

List of Figures

5.1 INTRODUCTION TO TRANSIENTS

Learning Objectives :

1. Given a transient curve:
   - At selected numbered points, explain what caused the parameter to change.
   - At selected numbered areas of the curve, explain why the parameter is trending in that area.
   - State the cause of the transient (initiating event).

2. Given a plant transient scenario, explain the behavior of selected plant parameters, control systems, and equipment for the time designated in the scenario.

5.1.1 Introduction

The following information is presented with the emphasis on analyzing given plant transients with respect to initiating conditions, transient events, end result and conclusions. The transient curves contained in this manual were compiled and analyzed by members of the NRC's Technical Training Division. They were produced from data supplied from the GE BWR/4 Simulator. Specific parameter responses of the simulator were recorded in a data file and converted into graphs with the use of Excel and Claris CAD computer programs. These graphs are **not** to be considered ***Engineering Simulator Model Quality***. Some minor editing of the original curves was performed.

The instructor explanations accompanying these curves are the result of analysis by the TTD Staff during the actual simulator runs and subsequent staff seminars.

Caution is advised when trying to apply these simulator curves to any operating plant. Even relative minor changes in set points, capacities, or piping runs could cause significant differences in indicated responses.

During analysis and study of the curves, the student should concentrate on explaining changes in various parameters caused by the initiating event, subsequent automatic operation of associated control systems or system response to the event. When explaining the identified points always try to relate cause and effect (e.g. power changing from flow change). Don't place too much emphasis on isolated portions of minor deviations in traces unless identified by the instructor.

5.1.2 Transients

In general, the term reactor transient applies to any significant deviation from the normal operating value of any of the key reactor operating parameters. Transients may occur as a consequence of an operator error or the malfunction or failure of equipment. Operational transients are divided into three groups: normal, abnormal and emergency. This division groups transients according to their relative severity on plant operations and safety.

5.1.2.1 Normal Operational Transient

Includes the events that take place during a normal plant startup, shutdown, or load change. These events do not take into effect equipment failure or operator error.

5.1.2.2 Abnormal Operational Transient

Anticipated (Abnormal) transients are deviations from the normal operating conditions that may occur one or more times during the service life of a plant. Anticipated transients range from trivial to significant in terms of the demands imposed on plant equipment. Anticipated transients include such events as a turbine trip, EHC failure, MSIV closure, loss of feedwater flow and loss of feedwater heating. More specifically, all situations (except for LOCAs) which could lead to fuel heat imbalances are anticipated (abnormal) transients.

Many transients are handled by the reactor control systems, which would return the reactor to its normal operating conditions. Others are beyond the capability of the reactor control systems and require reactor shutdown by the reactor protection system (RPS) in order to avoid damage to the reactor fuel or coolant systems.

5.1.2.3 Emergency Operational Transient Accident

An emergency operational transient (accident) is a single event, not reasonably expected during the course of plant operations, that has been hypothesized for analysis purposes or postulated from unlikely but possible situations, and that causes or threatens a rupture of a radioactive material barrier. A pipe rupture is an accident. A fuel clad defect is not.

Design Basis Accident

A design basis accident is a hypothesized accident, the characteristics of which are utilized in the design of those systems and components pertinent to the preservation of radioactive material boundaries and restriction of the release of radioactive materials from these boundaries. The potential radiation exposures resulting from these accidents is greater than any similar accident postulated from the same general assumptions. Design basis accidents include:

- control rod drop accident
- refueling accident
- main steam line break outside the drywell
- loss of coolant accident

5.1.3 Transients Analysis

Transient analysis begins with applying some fundamental rules:

1. Do not try and identify the initiating event.
2. Start with a parameter that you personally know more about.
3. Stay in the same time frame (i.e. do not continue on the same parameter trying to identify all the points prior to going to the next parameter).
4. Make a list of what would cause the parameter of interest to change.
5. Start with the first item on the list and decide what direction and how much of a change you would expect; then look at the change on the curve and see if it is reasonable.
6. If you are not sure continue down the list.
7. Go to the parameter that is affected by the one you have chosen (i.e. power effects pressure, pressure effects steam flow).
8. If you have done everything correctly you will end up with the initiating event.
9. Move to the next time frame and continue the process until all points are identified.
10. Test to see if all points agree with the initiating event.

Figures 5.1-1 represents a blank recorder paper. Each horizontal line is spaced 30 seconds apart and are the same for each parameter. The chart recorder moves from top to bottom, making the top 6 minutes and the bottom time zero.

The following are general notes applicable to all transients unless otherwise indicated:

- Reactor power is from one APRM channel. Assume that if this channel changes the other APRM channels also change.

- Total steam flow is from the FWCS's summations of the individual flow from the flow restrictors on each steam line.
- Total feedwater flow is from the FWCS's summed feed flow from the individual flow measurement devices down stream of the last high pressure feedwater heater.
- Total core flow is the summation of all of the jet pump flows.
- Turbine steam flow is the turbine first stage pressure converted to steam flow.
- Reactor pressure is from one of the reactor vessel pressure monitoring devices.

Transient one, in section 5.2, is a normal operational transient that will be used during the introduction for purposes of indicating how the various parameters change and the use of the rules identified above. ***All other transients covered will fall in the abnormal transient category***

5.1.3.1 Transient Example

Starting with reactor power (rule 2), make a list of things that could change reactor power.

1. Recirculation flow
   a. Pump speed change
   b. Tripping of a recirculation pump
2. Control rod movement
   a. normal rod movement
   b. scram
3. Loss of feedwater heating
4. Pressure increase/decrease
5. Standby liquid control system initiation

Starting with the first item, decide how power should change and how much, then look at the total core flow and APRM curves. At the same or near the same time frame it appears that everything matches, a change in total core flow caused a change in reactor power.

The next step is to move to the next parameter. By applying rule number 7, move to reactor pressure. But, before looking at reactor pressure, decide how pressure should change. If power decreases at a steady rate, pressure should also decrease at that same rate. Look at the pressure curve, it appears that indeed pressure is following reactor power as expected.

Applying rule number 7 again, if pressure changes, the EHC system should respond by adjusting the control and/or bypass valves. Adjusting control valves/BPVs will have an effect on main steam flow. So the next logical parameter is turbine steam flow, and to compare main steam flow to turbine steam flow.

Continuing this process should answer all the questions for the initial change. If you did not start with the parameter that changed first, the above procedure will bring you around to the initiating event. This process is used on each time frame of interest until all points are identified.

A synopsis of transient number one takes place in the following manner:

- Recirculation flow decreases due to the decrease in recirculation pump speed. The decrease in core flow results in a higher void fraction and a negative net core reactivity. The power decrease causes fuel temperature, moderator temperature, and the void fraction to decrease. This continues until the core net reactivity again equals zero. During this transient, the power decrease starts immediately after the core net $\Delta K/K < 0$.

- Power decreases below the steady state value due to the fuel time constant. Before the power generated in the fuel can effect moderator density, fuel temperature must change along with heat transfer to the coolant. The fuel in BWRs responds relatively slow with a time constant between 6 and 10 seconds.

- When reactor pressure decreases, due to the power decrease, the EHC system responds by closing down on the CVs to throttle reactor pressure decrease.

- Reactor water level increases due to the recirculation system removing less water from the annulus than is being supplied by the moisture separator, steam dryers and feedwater.

- Prior to a recirculation flow increase, reactor power increases due to the decrease in feedwater temperature. The increase in reactor power produces an increase in reactor pressure and subsequent increase in steam flow, both total and turbine.

- Following the power decrease with flow, recirculation pump speed is returned to its original value, causing power to increase.

- The increase in reactor power produces a corresponding increase in reactor pressure.

- The increase in reactor pressure is sensed by the EHC system which responds by throttling open the turbine control valves.

- The increase in steam flow is monitored by the feedwater control system along with the level decrease and adjust feedwater flow to maintain reactor water level.

- The decrease in reactor level is caused by the steam flow/feedwater flow mismatch and the recirculation system removing a larger volume of water from the annulus area.

Table 5.1-1 Parameter Setpoint Aids

	Reactor Vessel Level (inches)
Level 8 (56.5)	Trip of main turbine, RFP, RCIC, and HPCI
Level 7 (40.5)	High level alarm
Level 4 (33)	Low level alarm, permissive for Recirc pump runback to 45%
Level 3 (12.5)	Reactor scram, Recirc pump runback to 30%, ADS signal, RHR Isolation signal
Level 2 (-38)	Initiate RCIC and HPCI, ATWS- RPT, RWCU isolation and other seleceted systems
Level 1 (-132.5)	Initiate CS and LPCI, Start EDG, ADS signal, Isolate MSIVs
	Reactor Pressure (psig)
50	RCIC Isolation
100	HPCI Isolation
338 & 465	Permissive for injection of LPCI and CS
Main Steam Line pressure of 825 psig closes MSIVs	
920 - 1005	Normal reactor Pressure
1025	High pressure alarm
1043	Reactor Scram
1115/1125/1135	4/4/3 SRVs opening pressures
1120	ATWS - RPT
	Condenser Vacuum (inches of Hg)
22.5	Turbine trip
20.0	RFP trip
8.5	MSIV closure
7	BPV closure
	Turbine First Stage Pressure Usage
	Bypass EOC-RPT and Scram if <30%
	Drywell Pressure (psig)
1.0	High pressure alarm
1.69	Initate HPCI, CS and RHR, Start D/G and RBSVS, isolation signal for selected plant systems

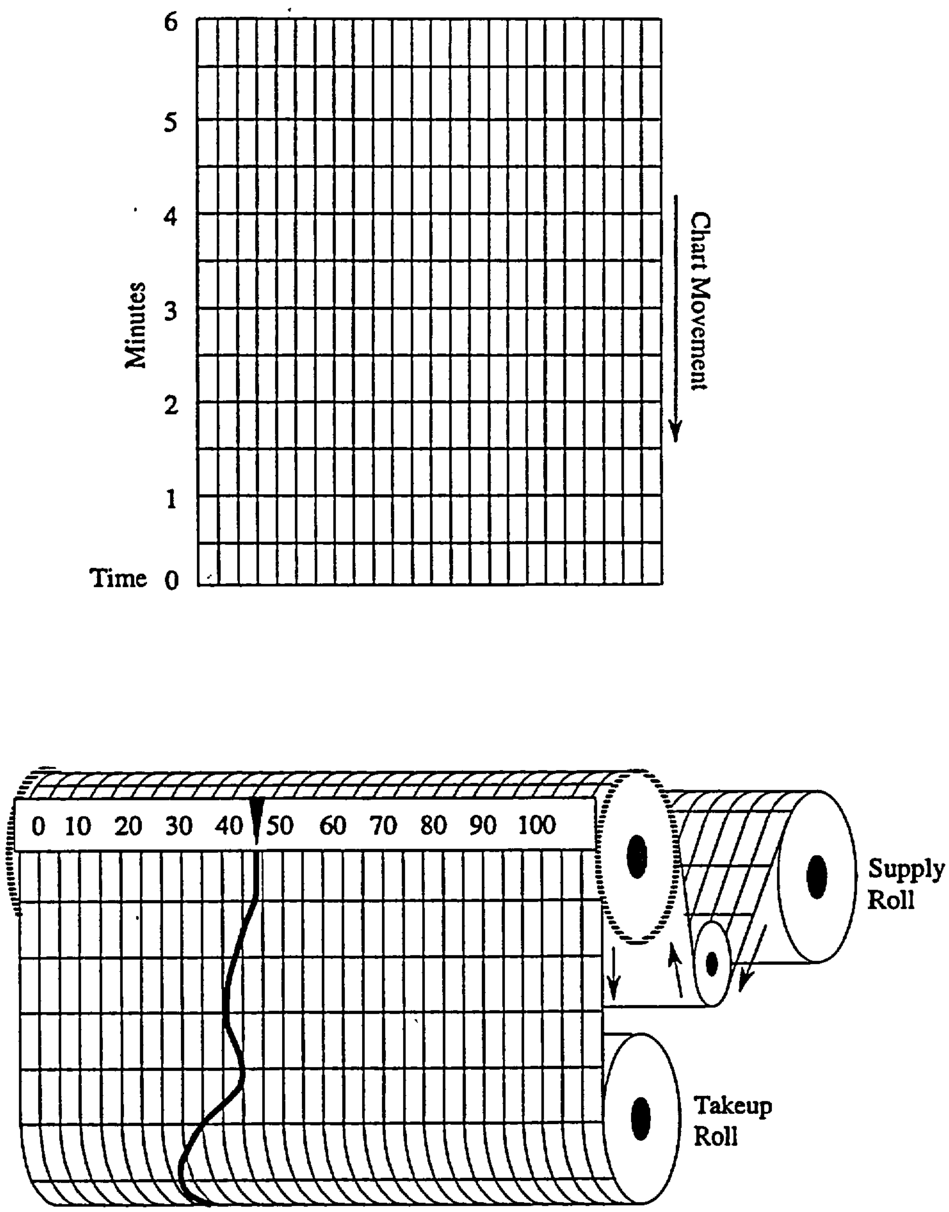


Chart Recorder

Figure 5.1-1 Chart Recorder

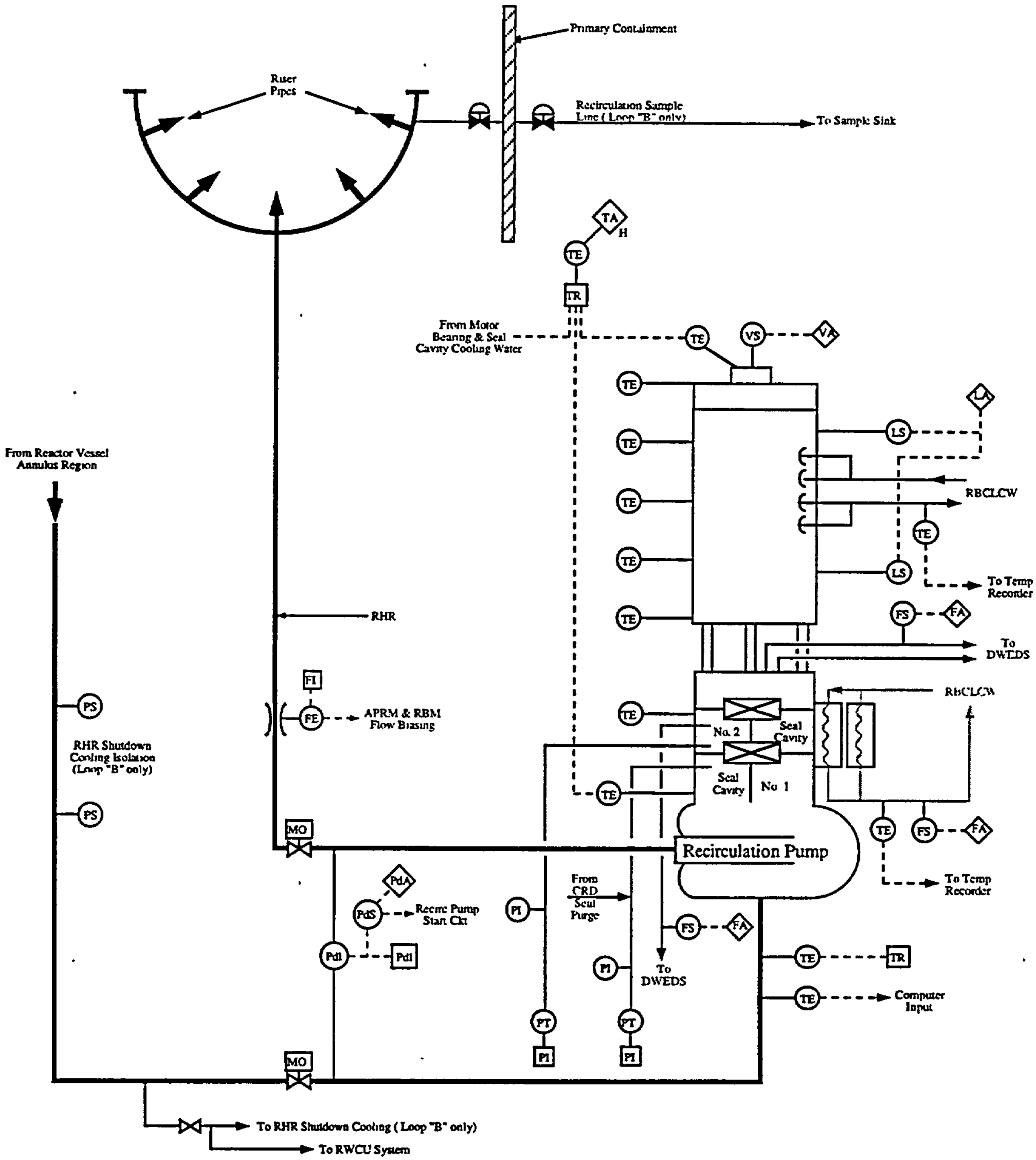


Figure 5.1-2 Recirculation Loop Instrumentation

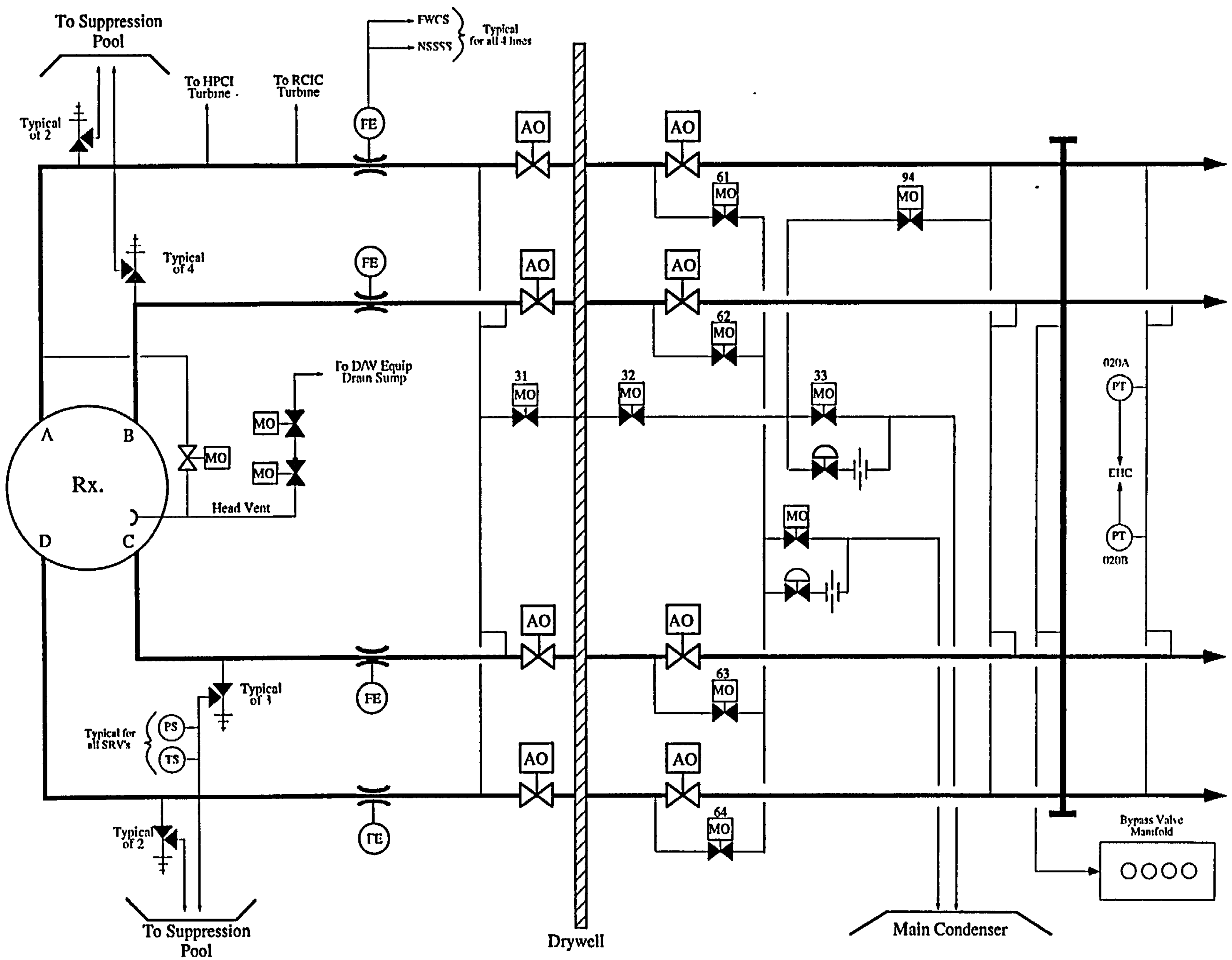


Figure 5.1-3 Main Steam System

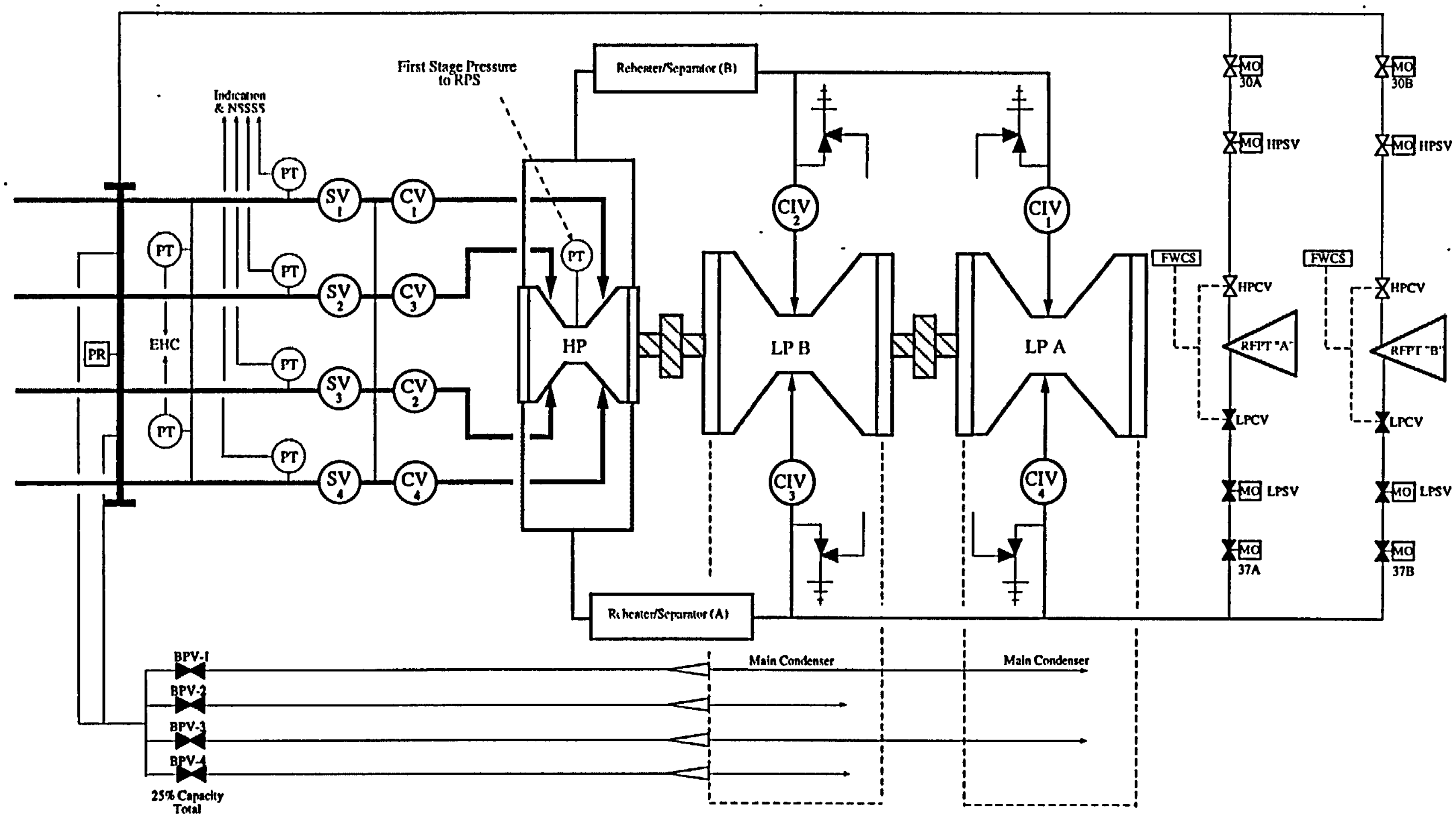


Figure 5.1-4 Main Steam System (Cont.)

1294

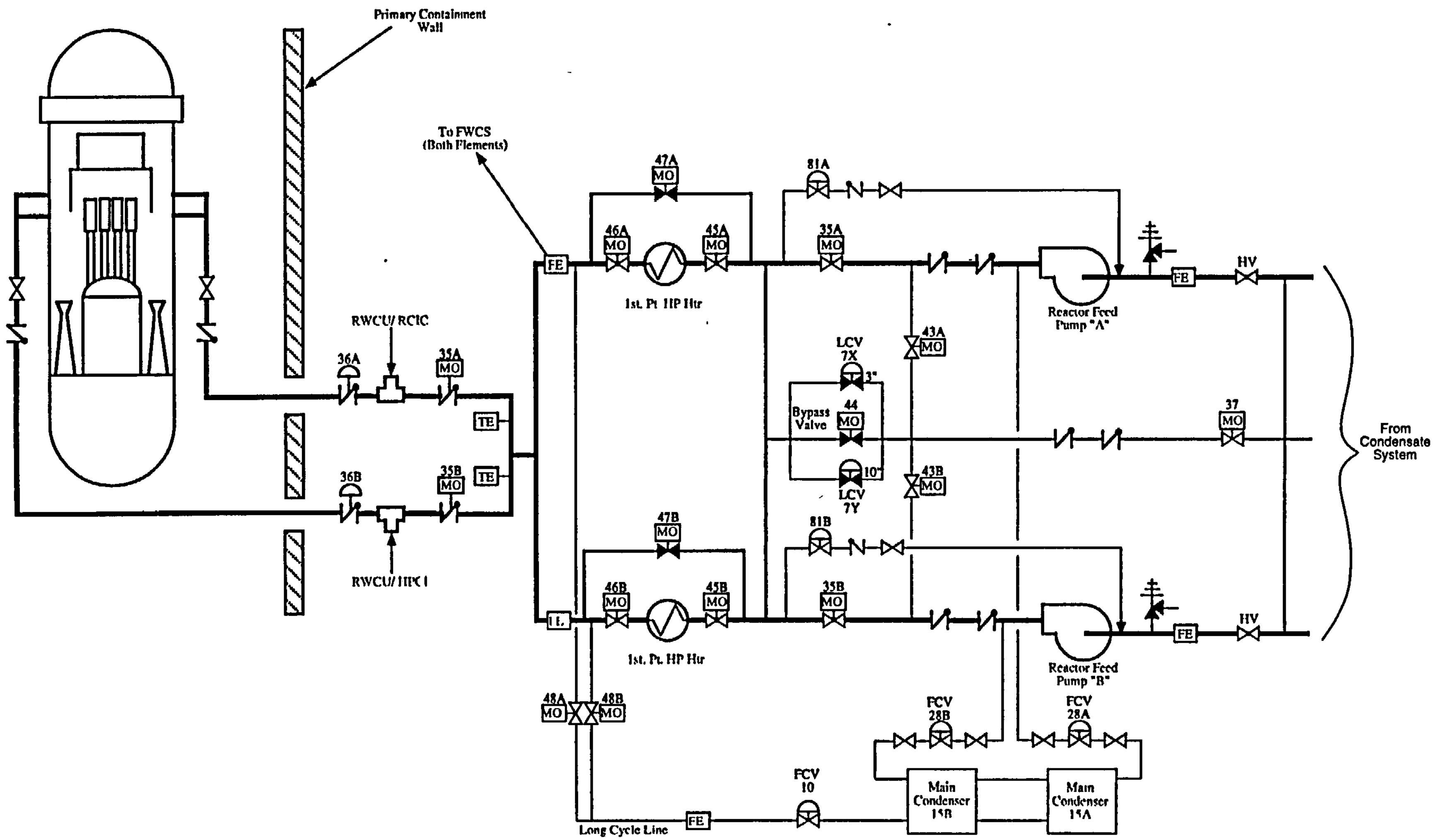


Figure 5.1-5 Feedwater System

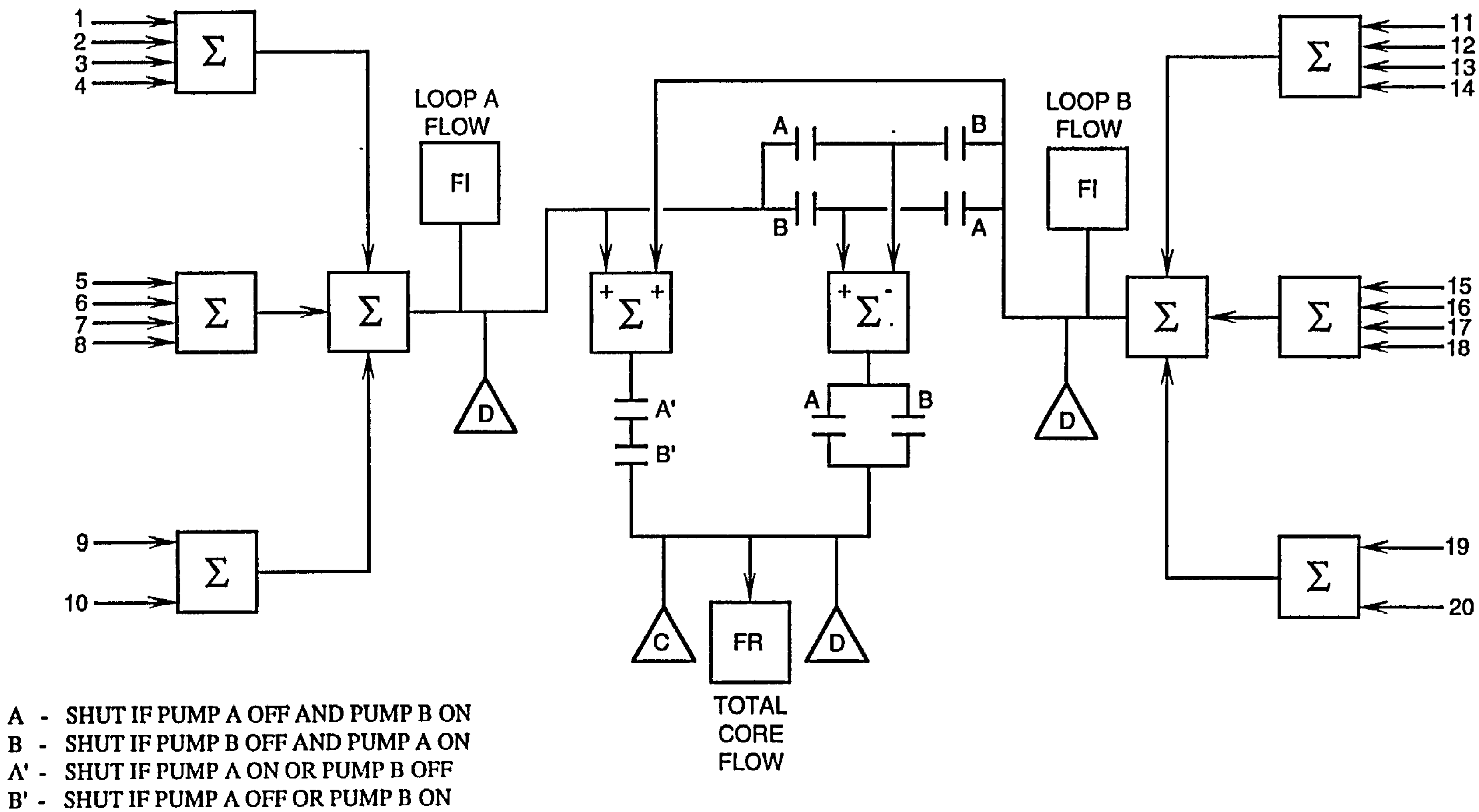


Figure 5.1-6 Core Flow Summing Network

0397-3

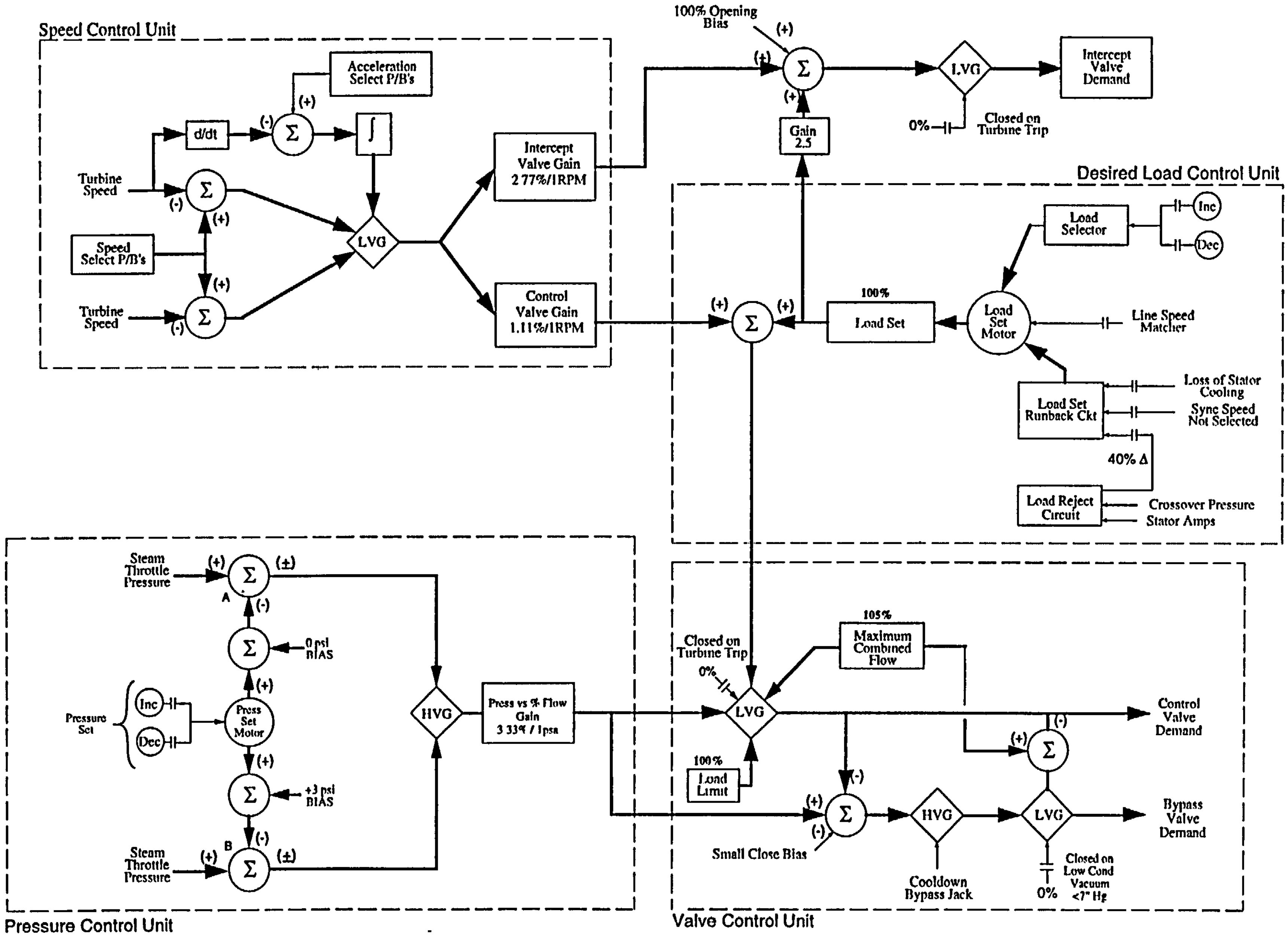


Figure 5.1-7 Electro Hydraulic Control System Logic

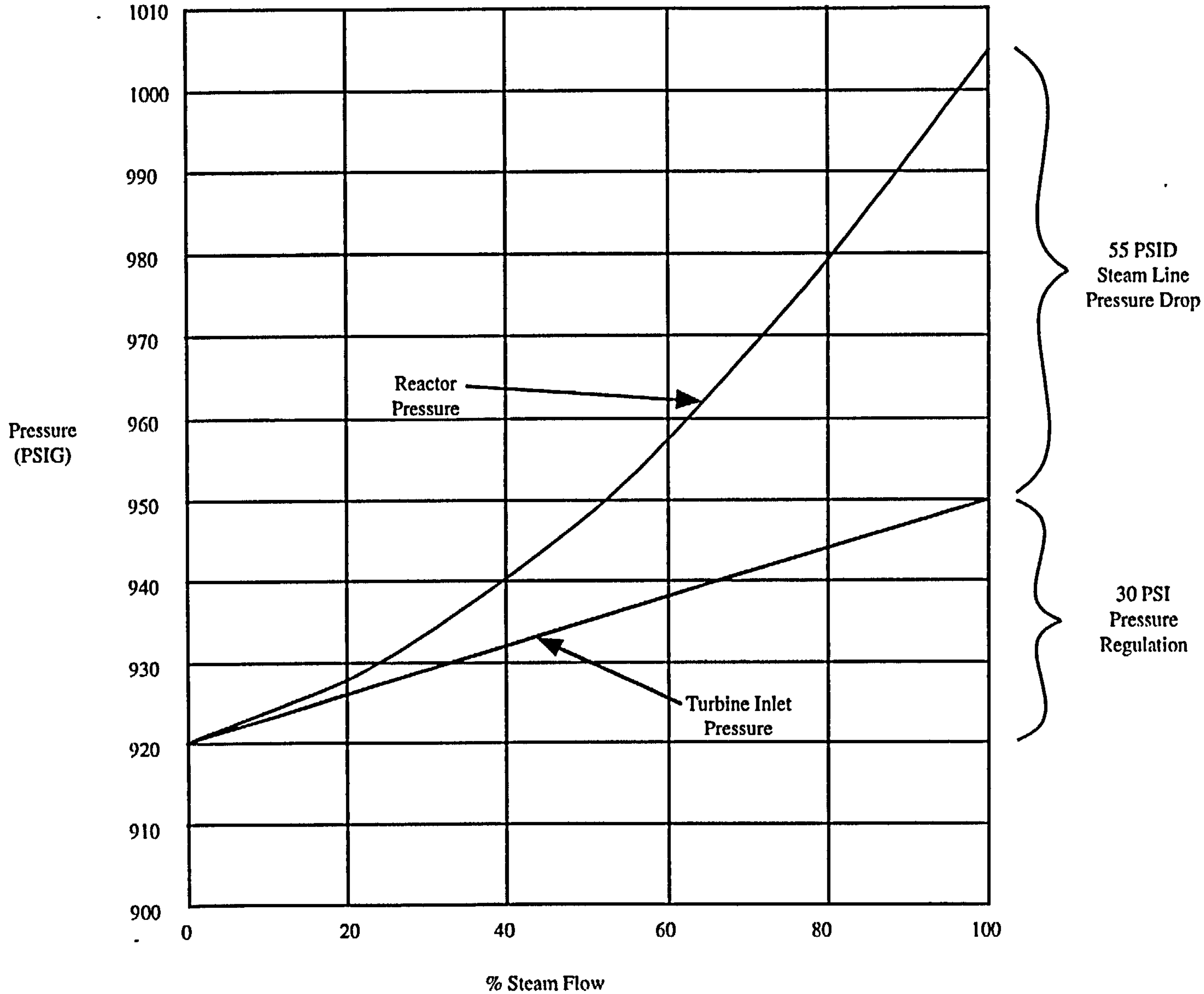


Figure 5.1-8 Pressure Control Spectrum

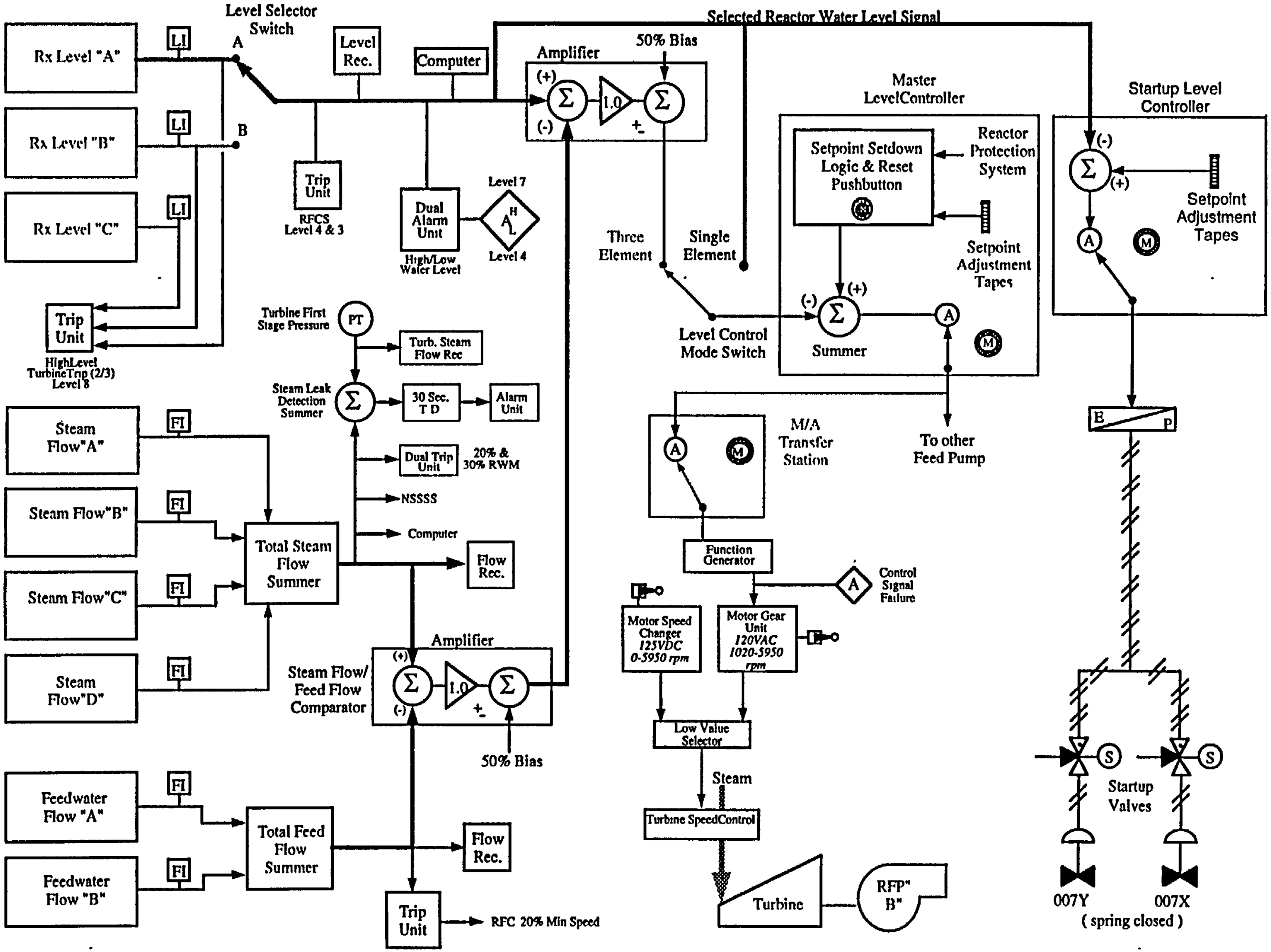


Figure 5.1-9 Feedwater Control System

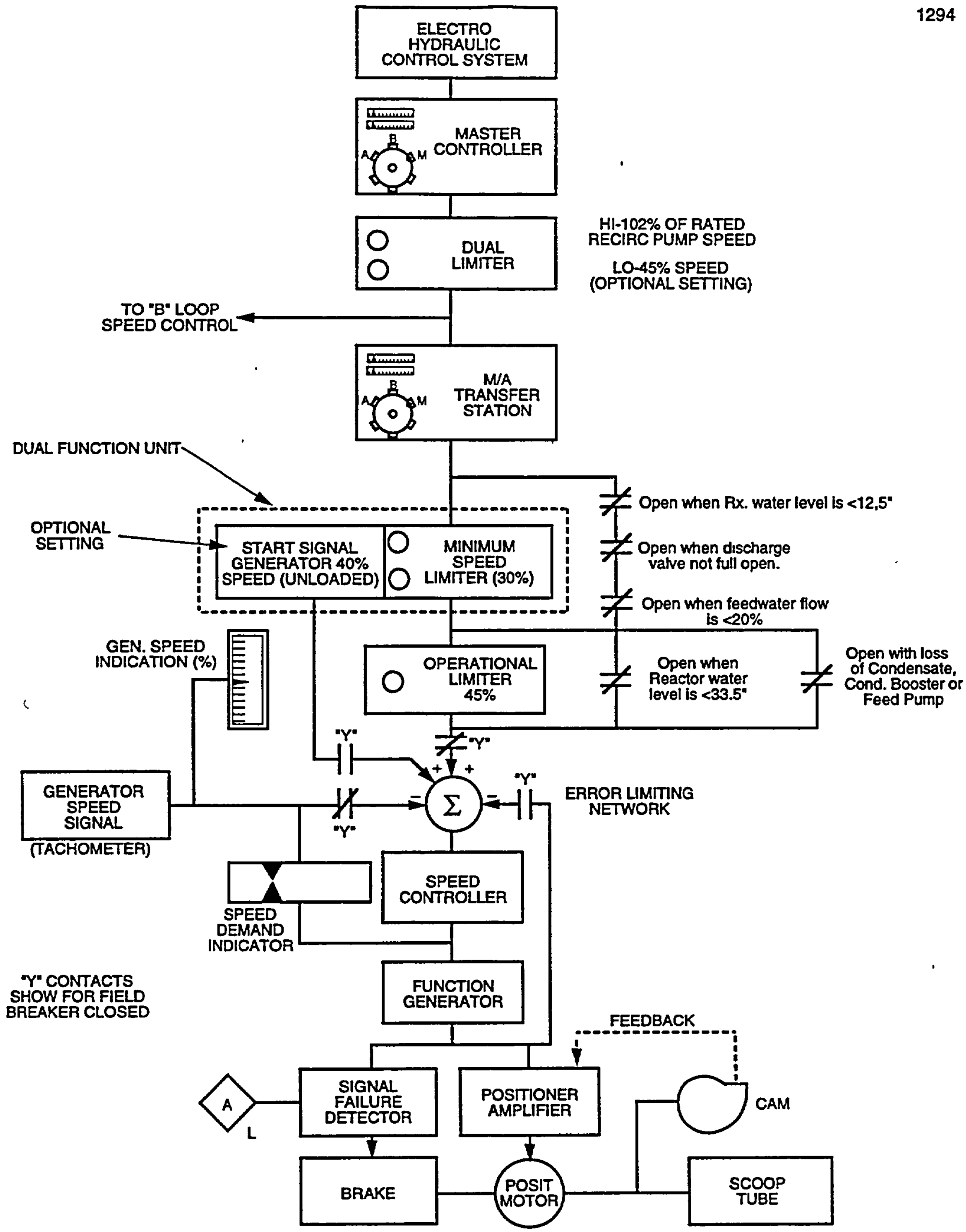


Figure 5.1-10 Recirculation System Flow Control Network
(Shown for A loop, TYP. for B)

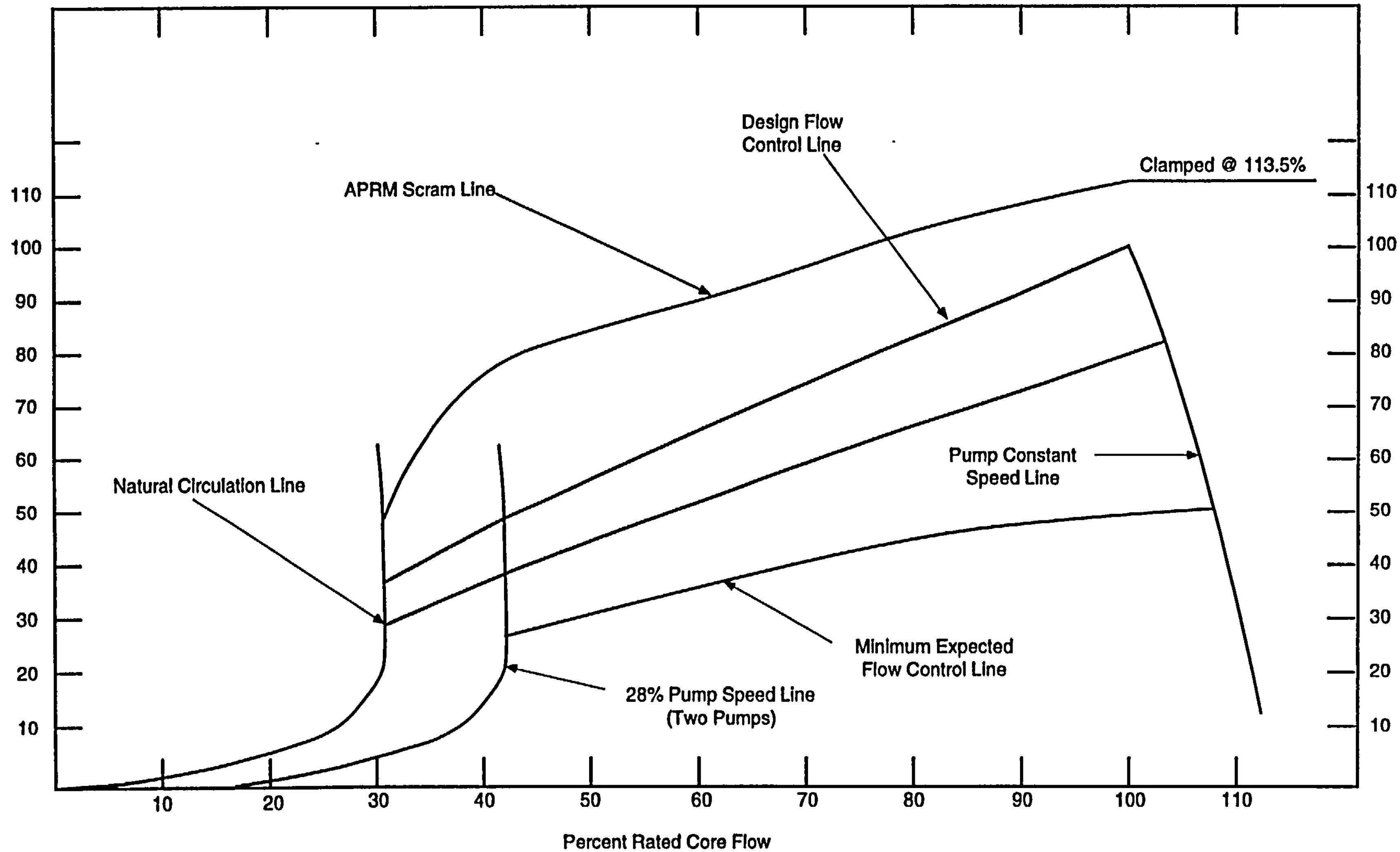
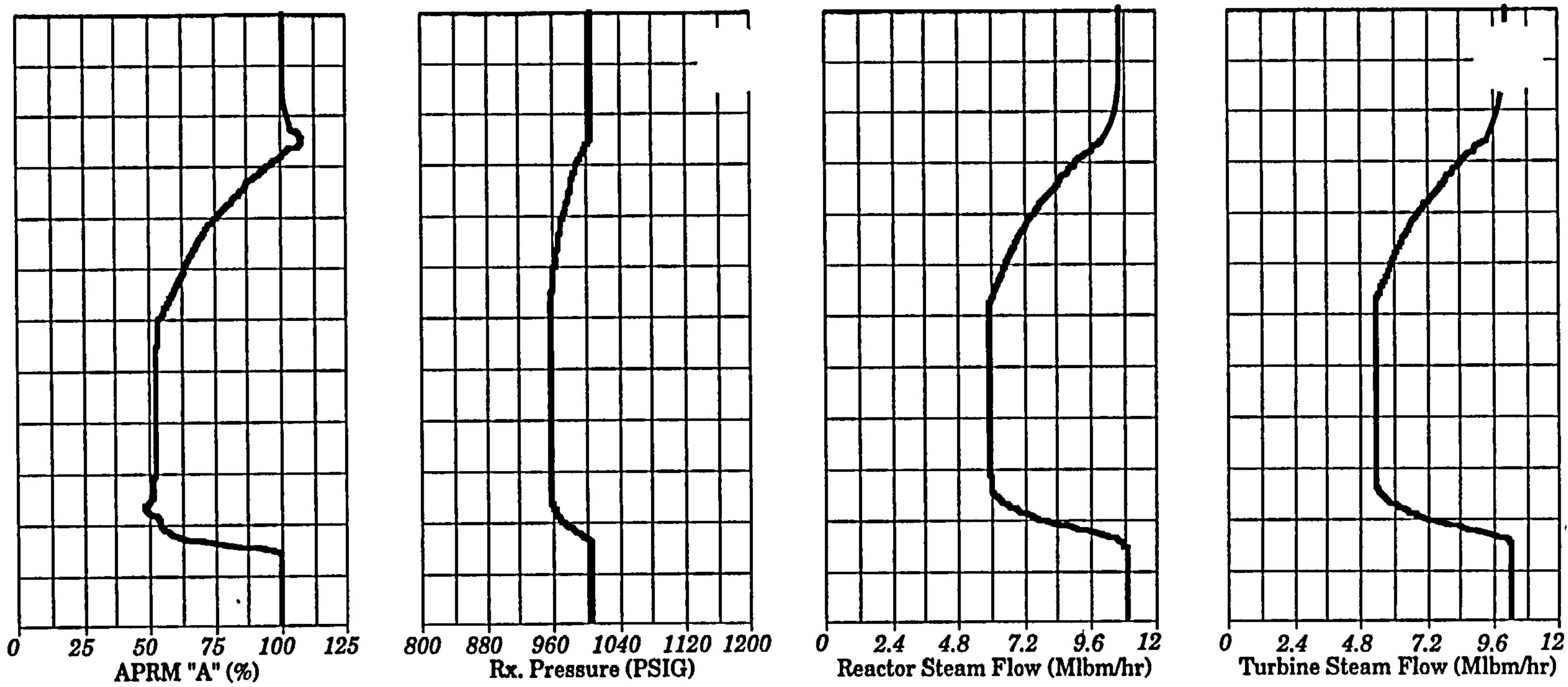
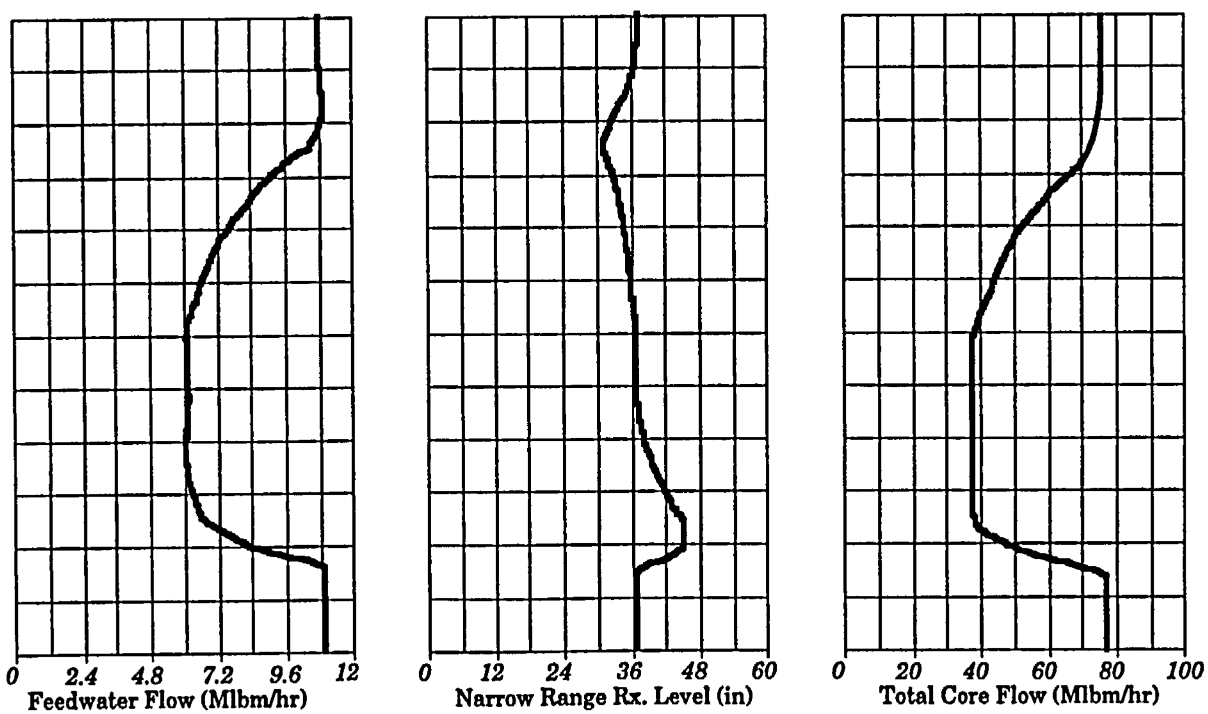


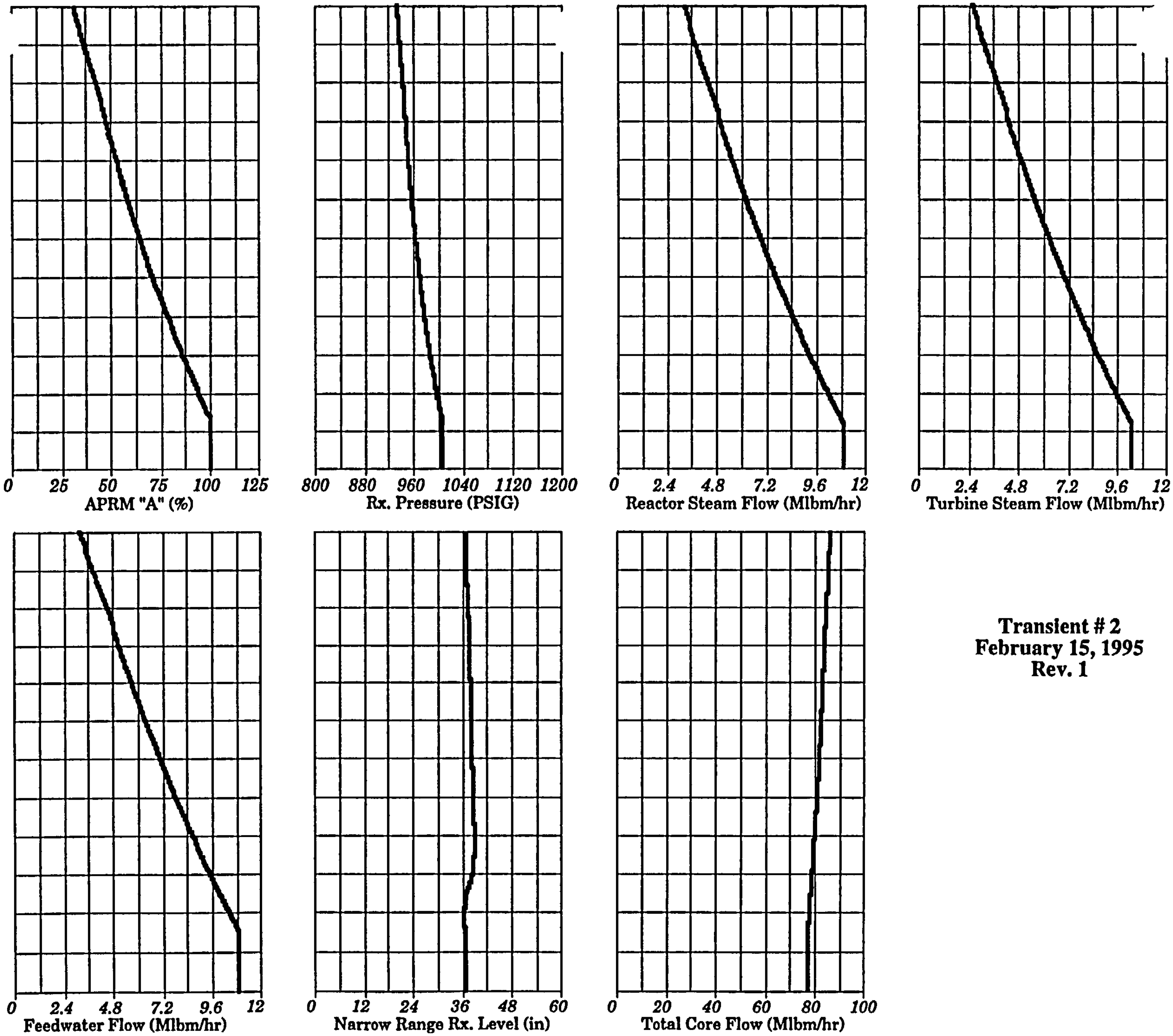
FIGURE 5.1-11 Power/Flow Map

0295

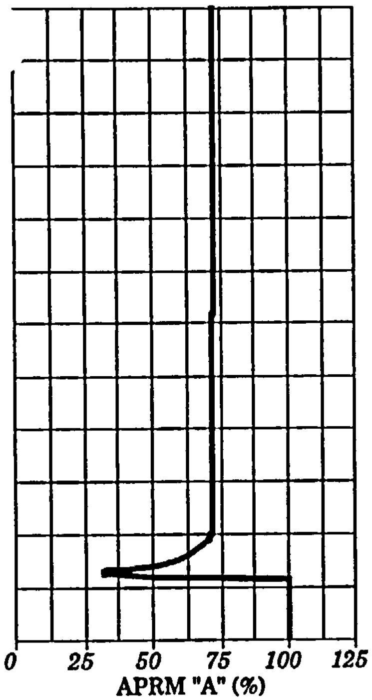


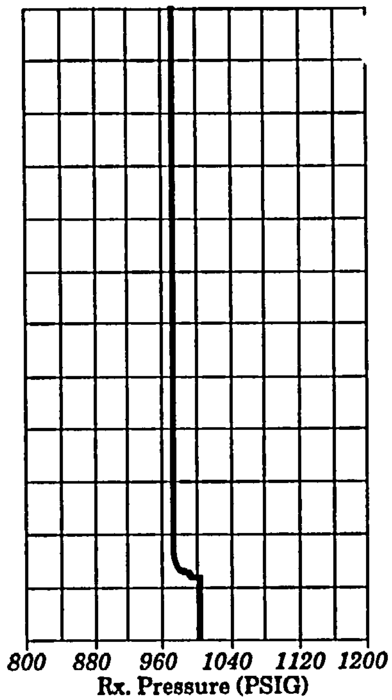


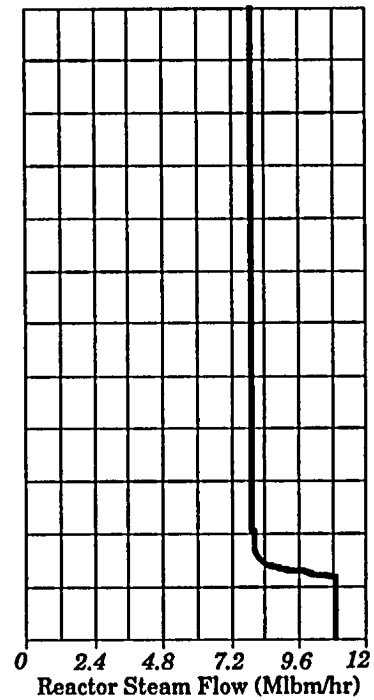
Transient #1
Febraury 15, 1995
Rev. 1

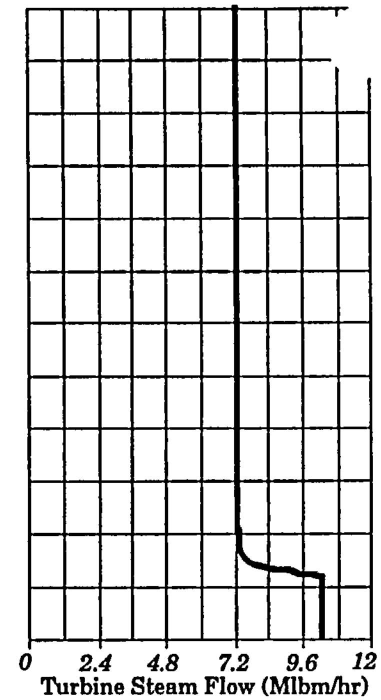


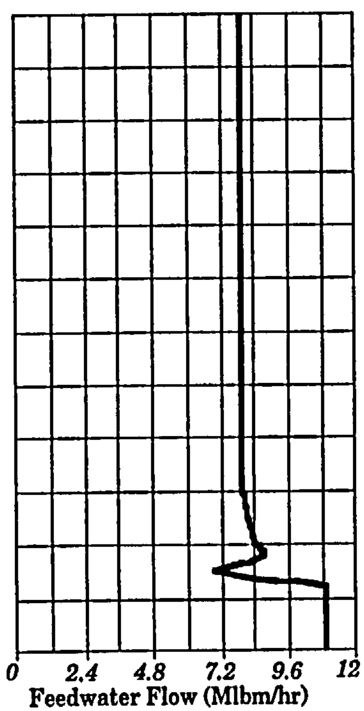
Transient # 2
February 15, 1995
Rev. 1

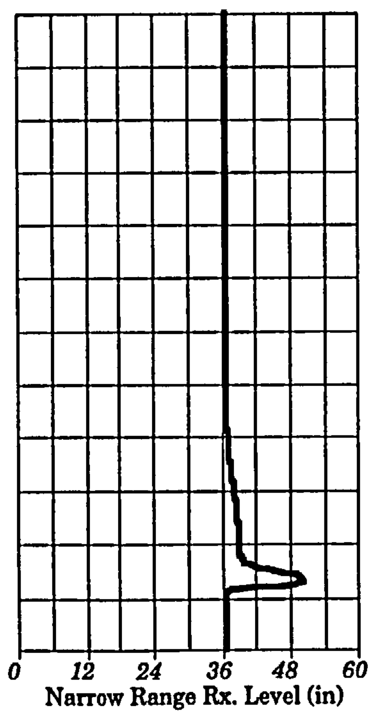


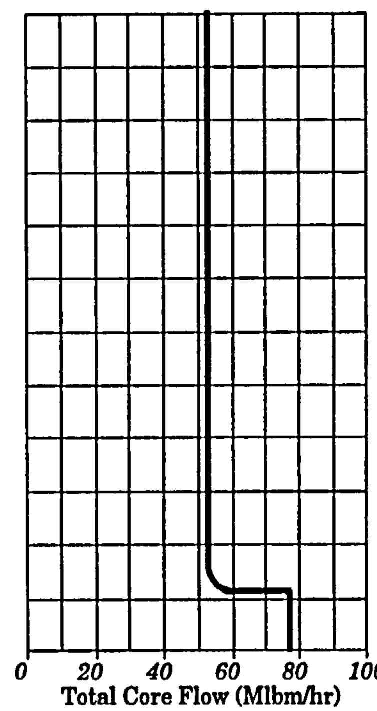






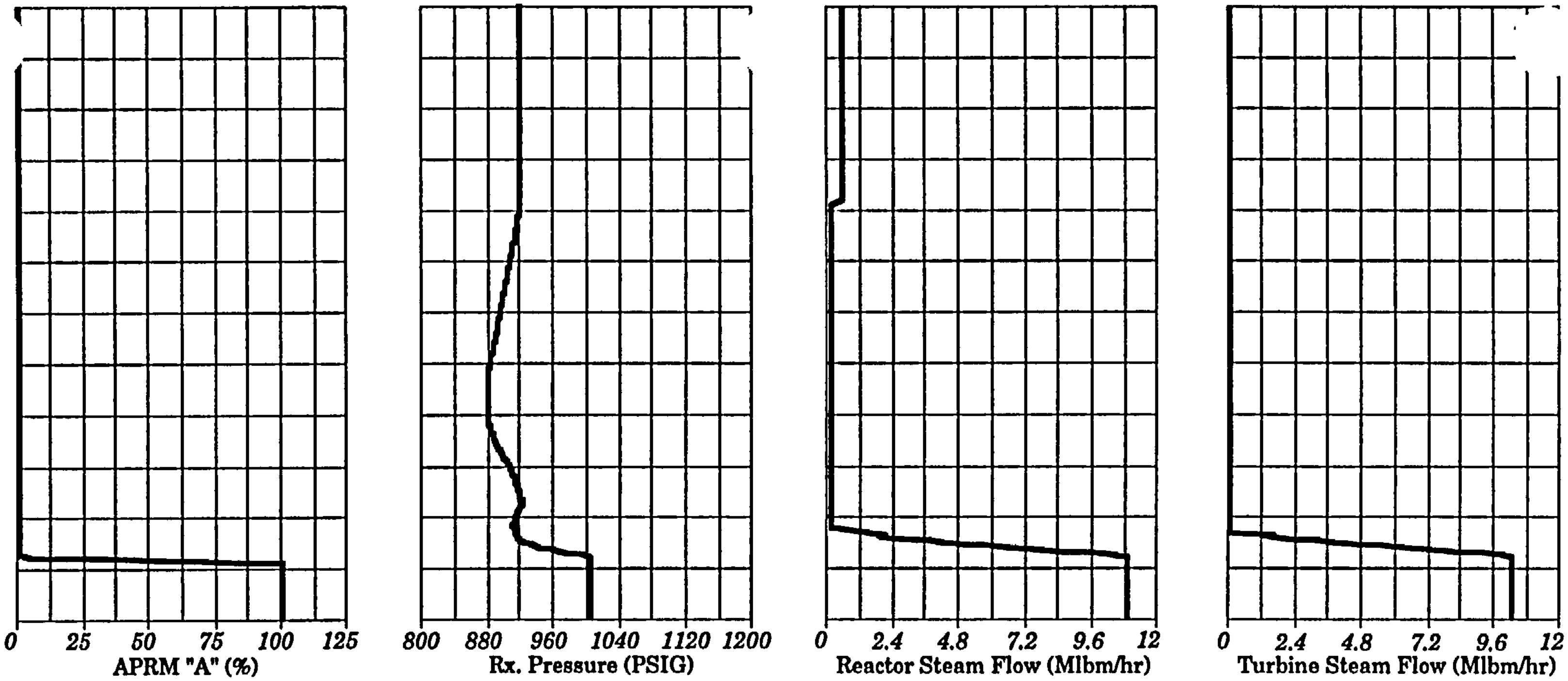


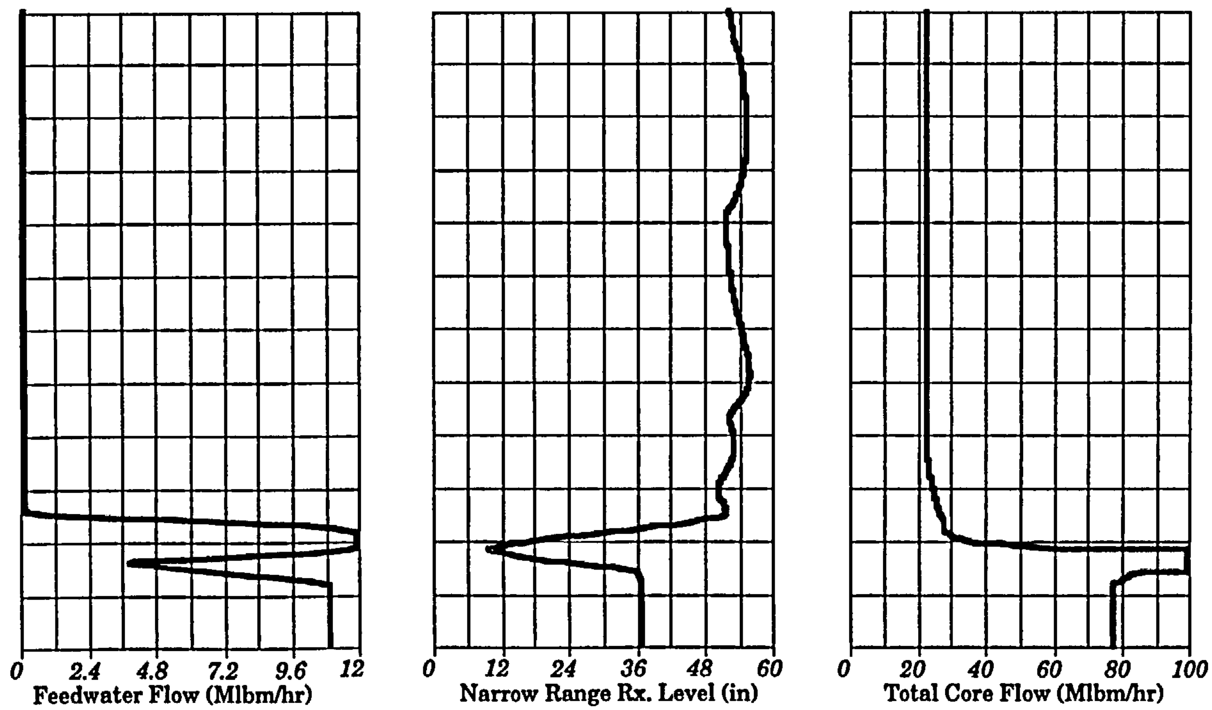




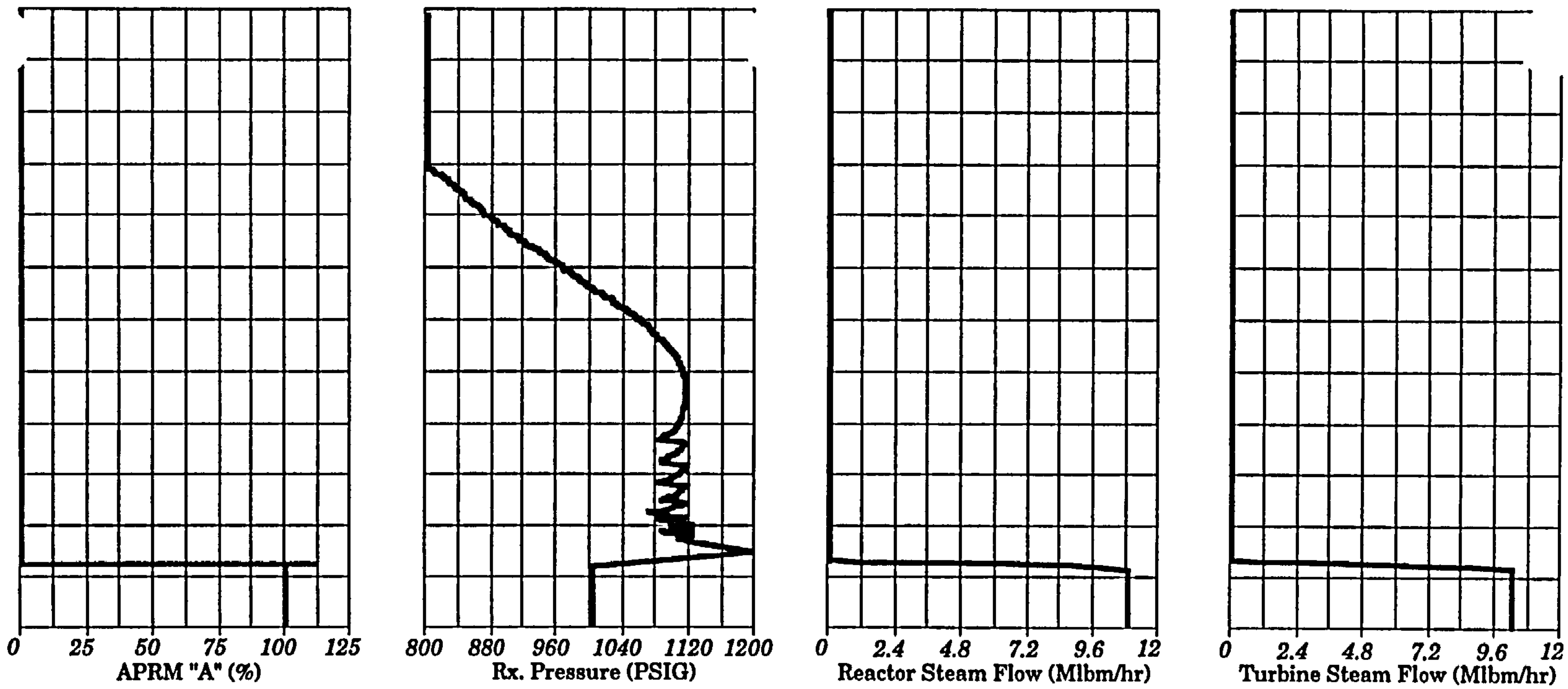
Transient #3

February 15, 1995
Rev. 1

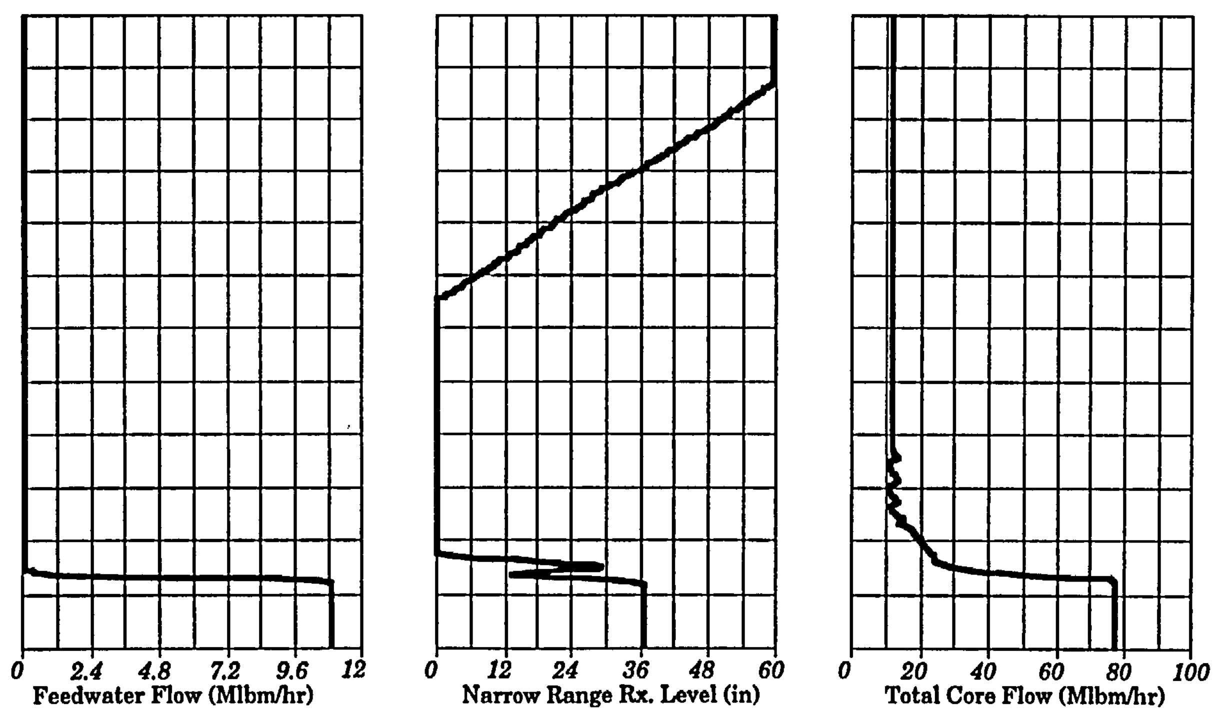




Transient #4
February 15, 1995
Rev. 1

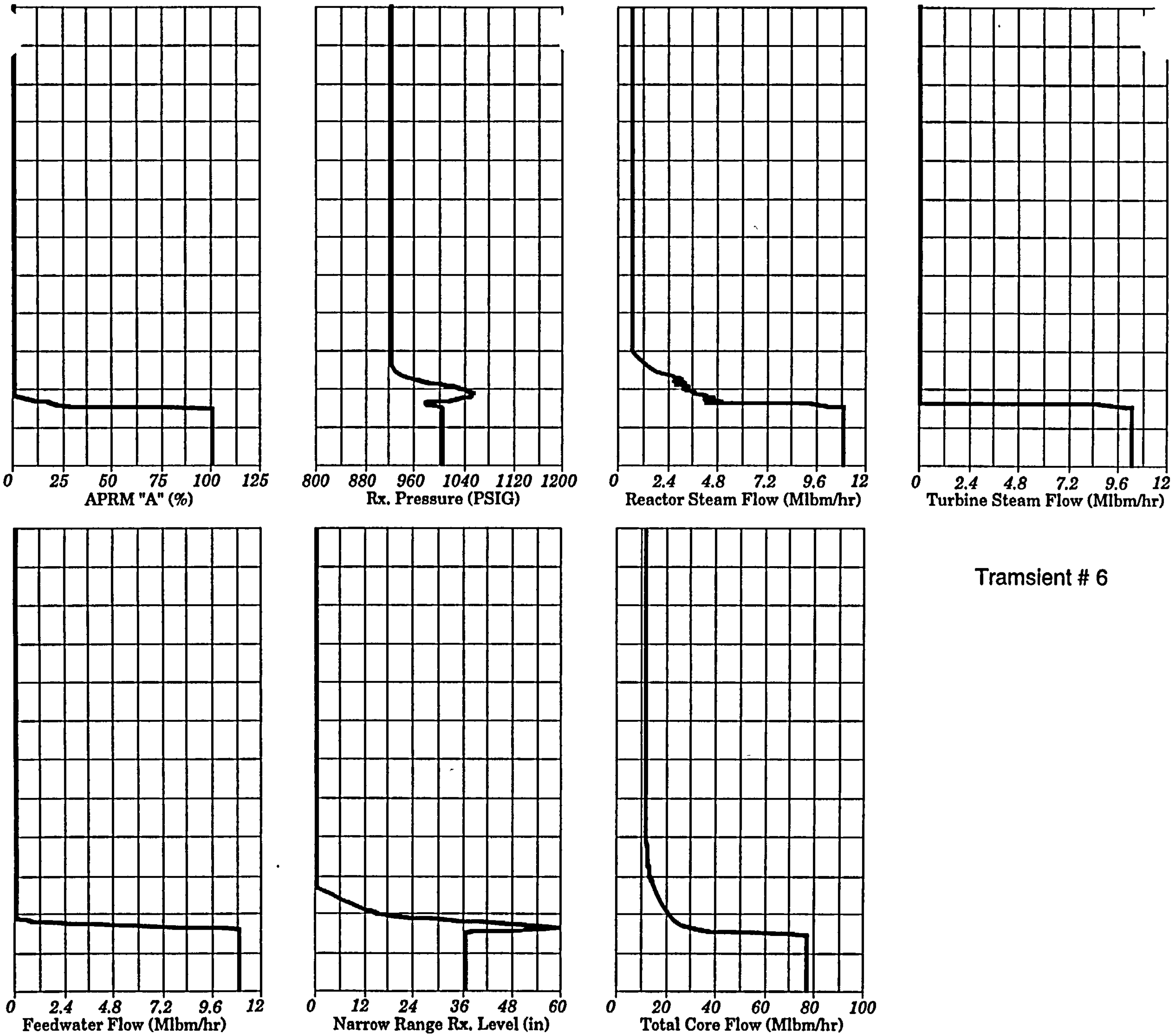


0 25 50 75 100 125
APRM "A" (%)
800 880 960 1040 1120 1200
Rx. Pressure (PSIG)
0 2.4 4.8 7.2 9.6 12
Reactor Steam Flow (Mlbm/hr)
0 2.4 4.8 7.2 9.6 12
Turbine Steam Flow (Mlbm/hr)

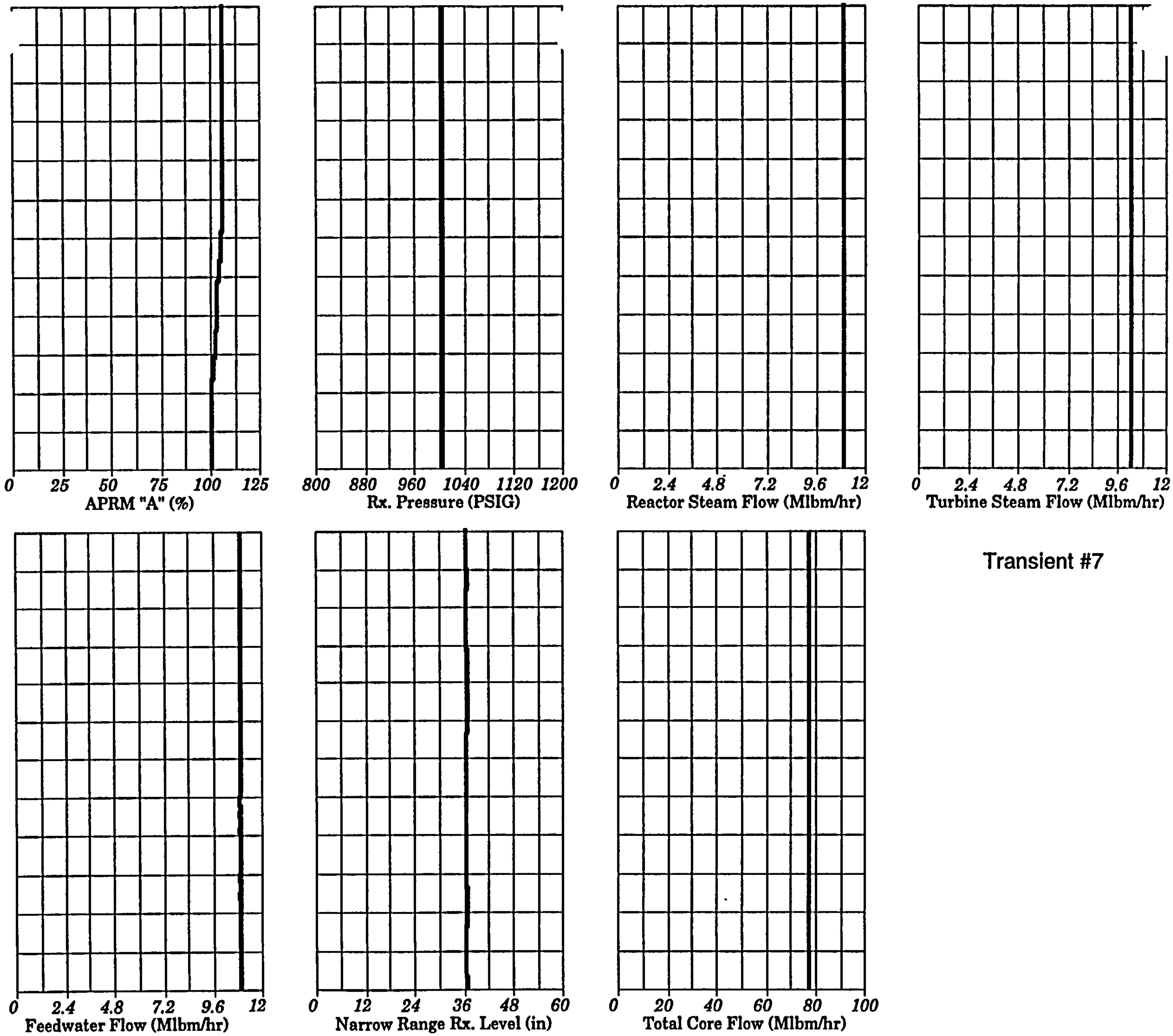


0 2.4 4.8 7.2 9.6 12
Feedwater Flow (Mlbm/hr)
0 12 24 36 48 60
Narrow Range Rx. Level (in)
0 20 40 60 80 100
Total Core Flow (Mlbm/hr)

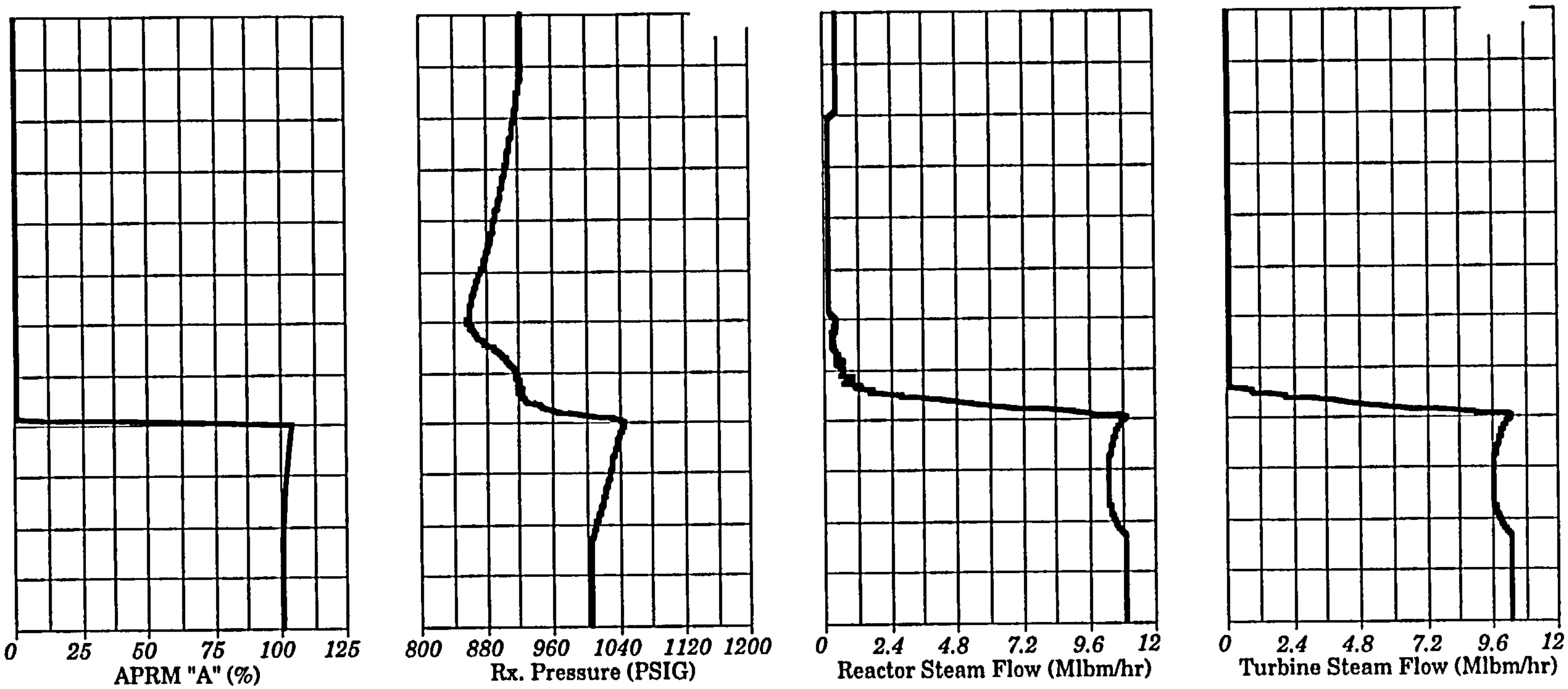
Transient #5

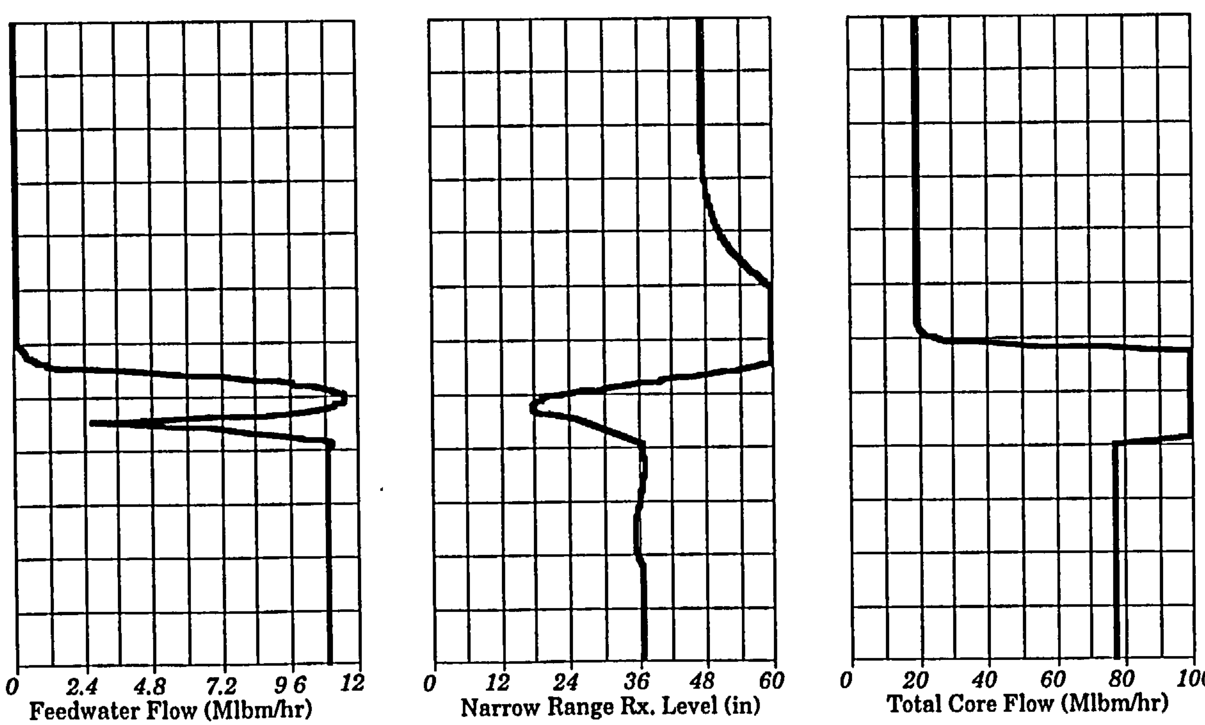

0 25 50 75 100 125
APRM "A" (%)
800 880 960 1040 1120 1200
Rx. Pressure (PSIG)
0 2.4 4.8 7.2 9.6 12
Reactor Steam Flow (Mlbm/hr)
0 2.4 4.8 7.2 9.6 12
Turbine Steam Flow (Mlbm/hr)
0 2.4 4.8 7.2 9.6 12
Feedwater Flow (Mlbm/hr)
0 12 24 36 48 60
Narrow Range Rx. Level (in)
0 20 40 60 80 100
Total Core Flow (Mlbm/hr)

Tramsient # 6

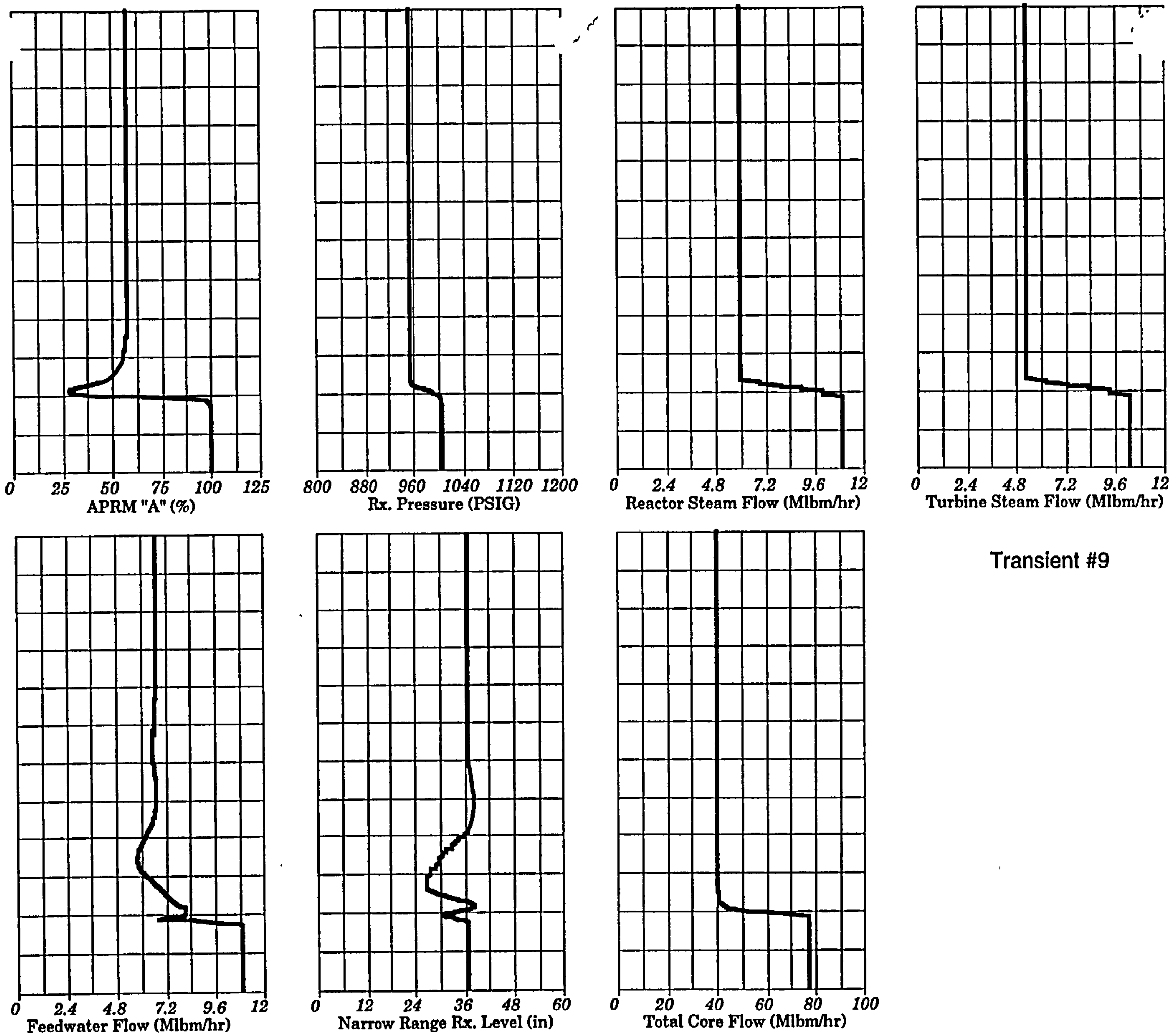

0 25 50 75 100 125
APRM "A" (%)
800 880 960 1040 1120 1200
Rx. Pressure (PSIG)
0 2.4 4.8 7.2 9.6 12
Reactor Steam Flow (Mlbm/hr)
0 2.4 4.8 7.2 9.6 12
Turbine Steam Flow (Mlbm/hr)
0 2.4 4.8 7.2 9.6 12
Feedwater Flow (Mlbm/hr)
0 12 24 36 48 60
Narrow Range Rx. Level (in)
0 20 40 60 80 100
Total Core Flow (Mlbm/hr)

Transient #7

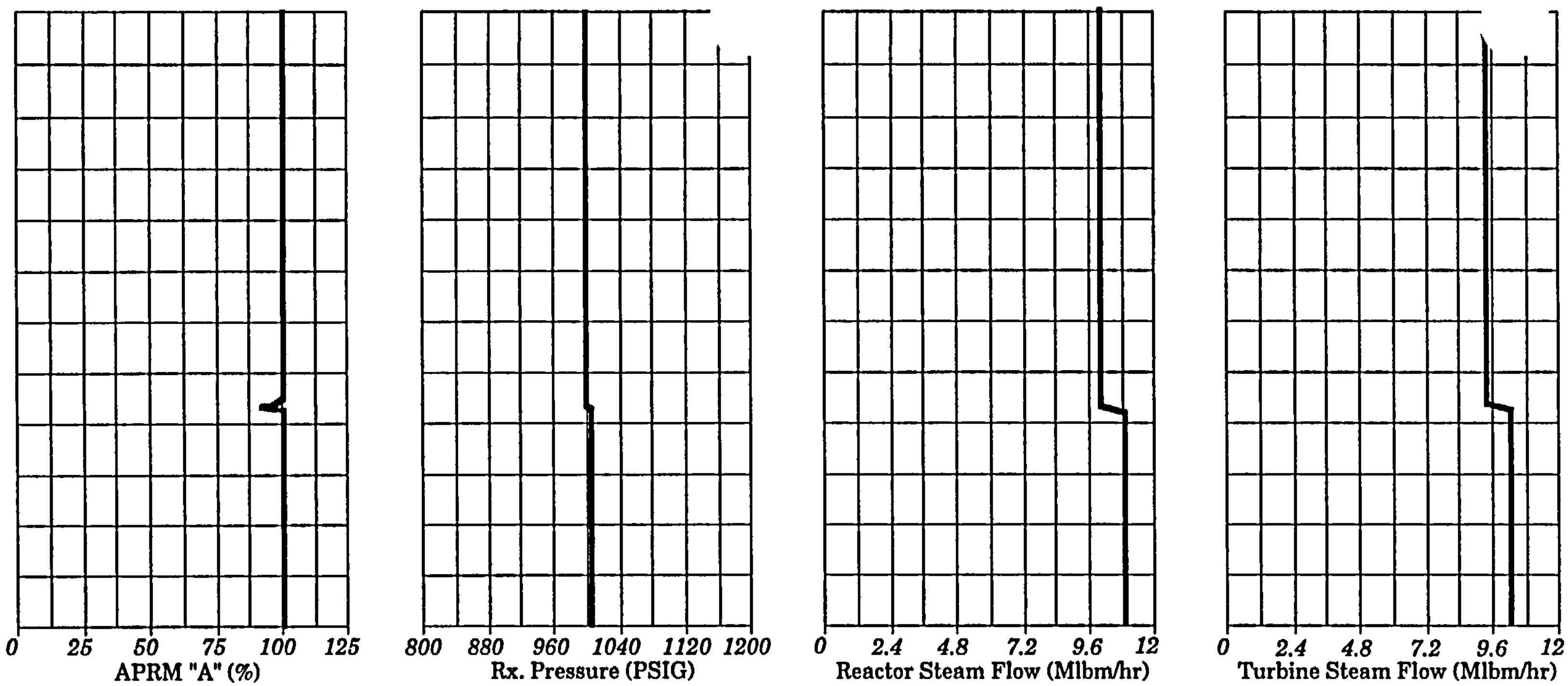


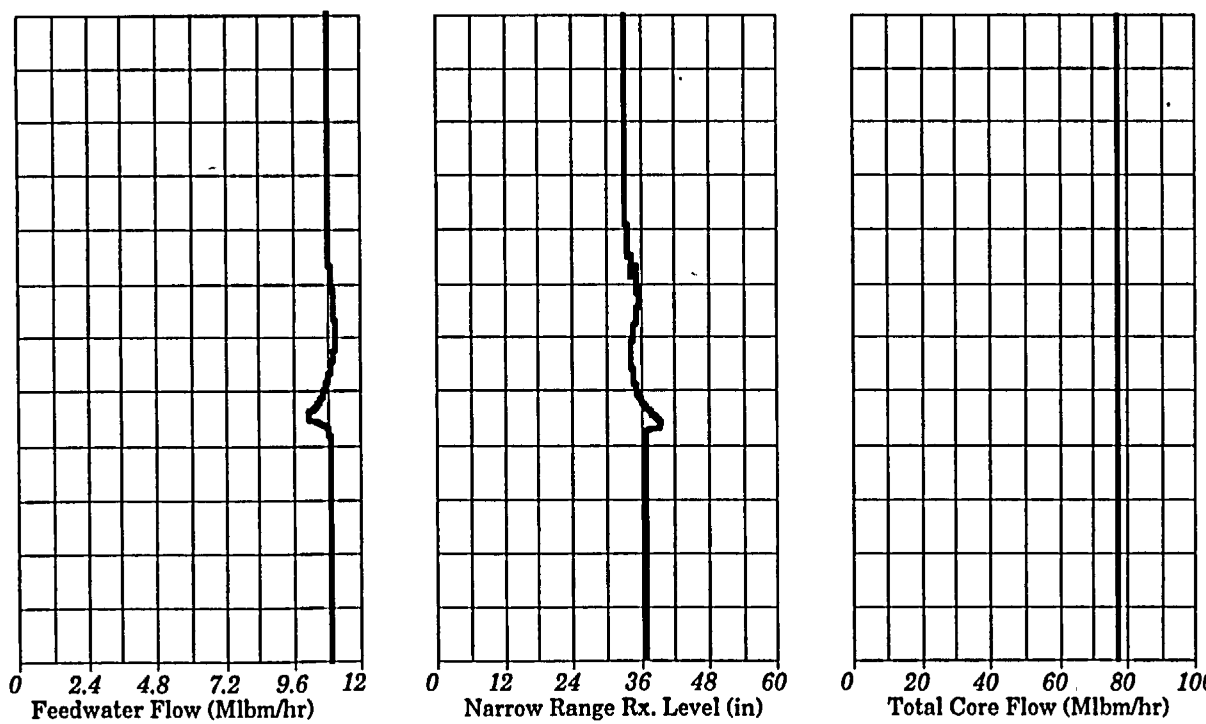


Transient #8
May 03, 1998
Rev. 1


0 25 50 75 100 125
APRM "A" (%)
800 880 960 1040 1120 1200
Rx. Pressure (PSIG)
0 2.4 4.8 7.2 9.6 12
Reactor Steam Flow (Mlbm/hr)
0 2.4 4.8 7.2 9.6 12
Turbine Steam Flow (Mlbm/hr)
0 2.4 4.8 7.2 9.6 12
Feedwater Flow (Mlbm/hr)
0 12 24 36 48 60
Narrow Range Rx. Level (in)
0 20 40 60 80 100
Total Core Flow (Mlbm/hr)

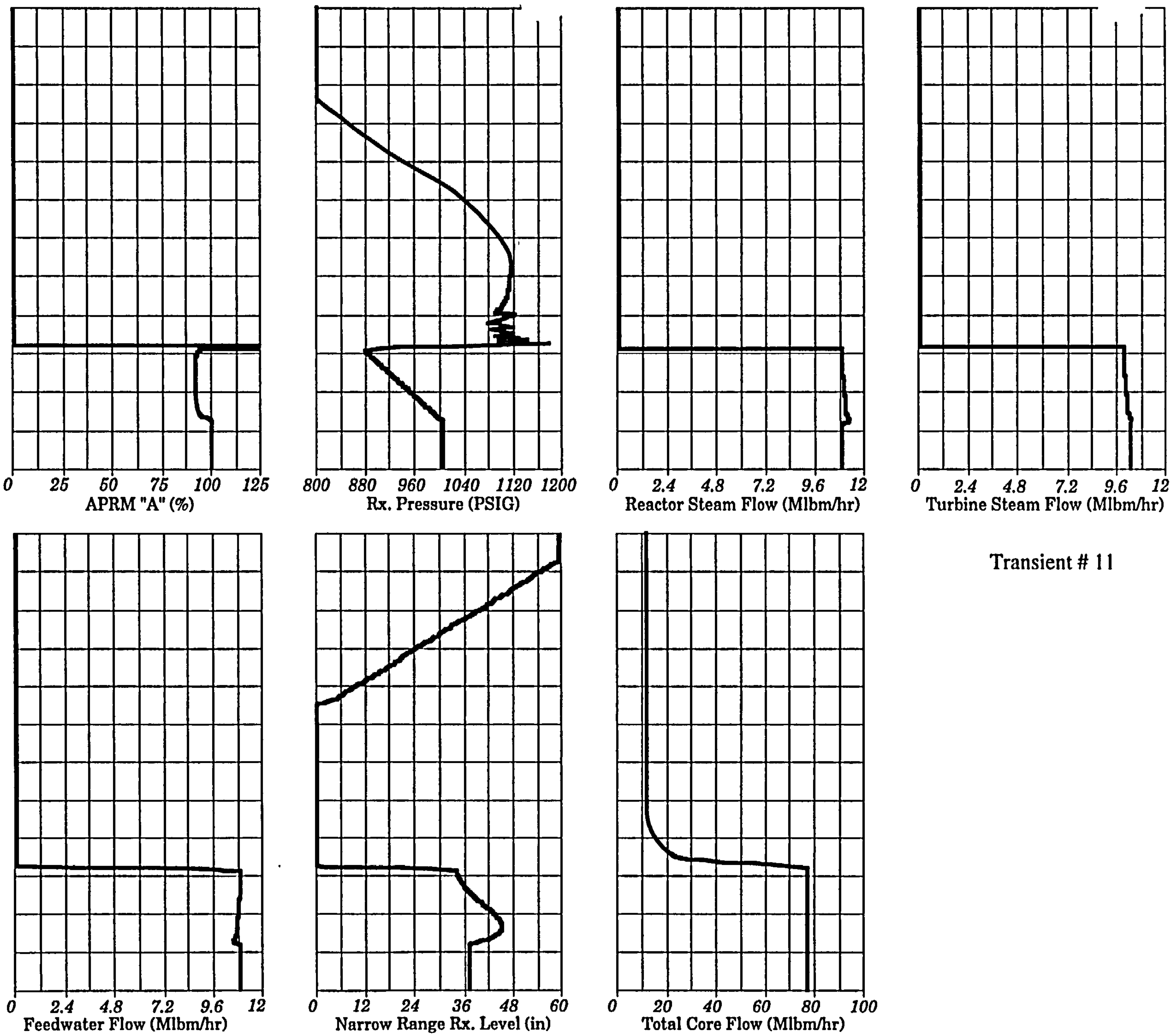
Transient #9



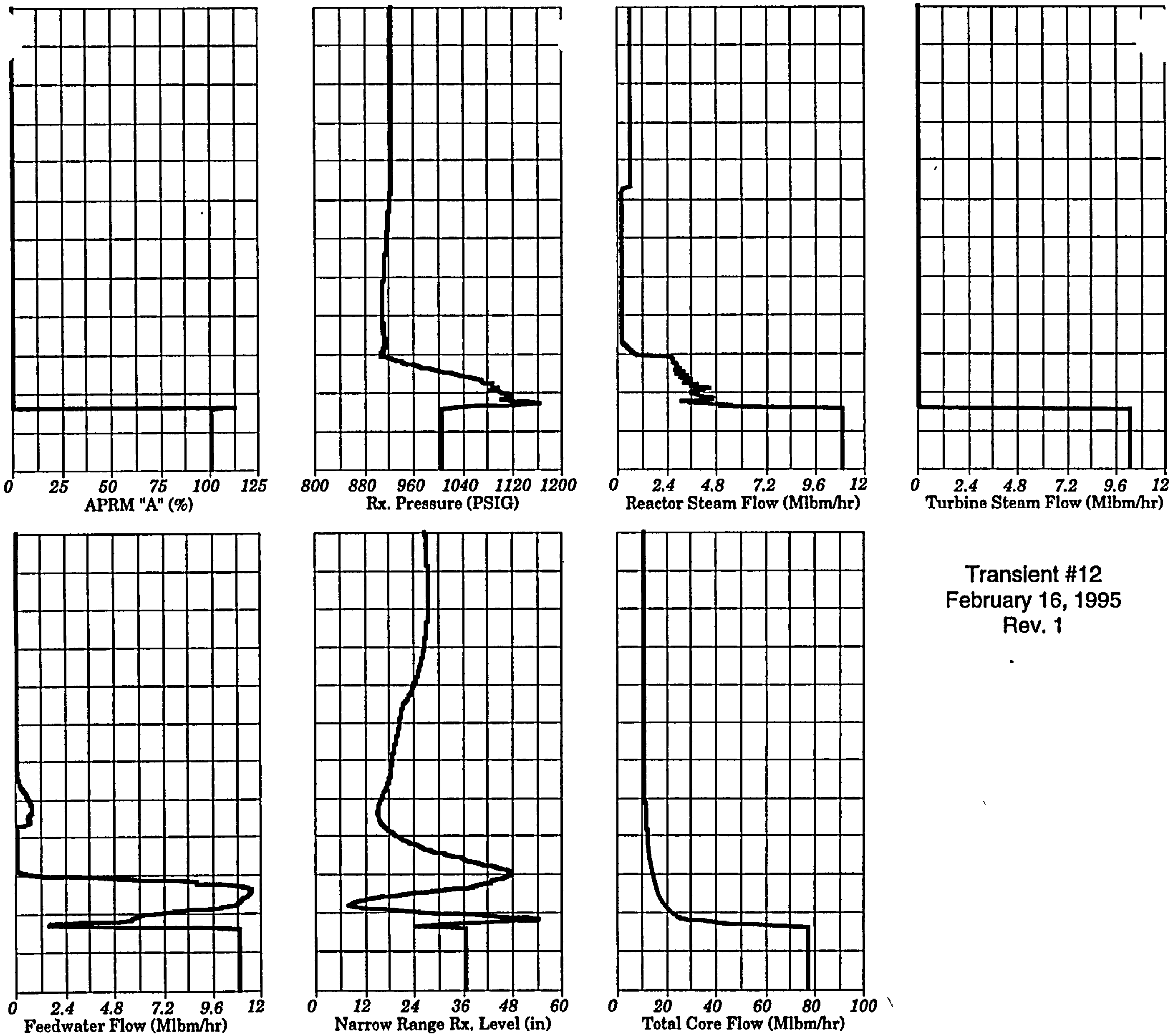


Transient #10
February 15, 1995
Rev. 1

Transient #10

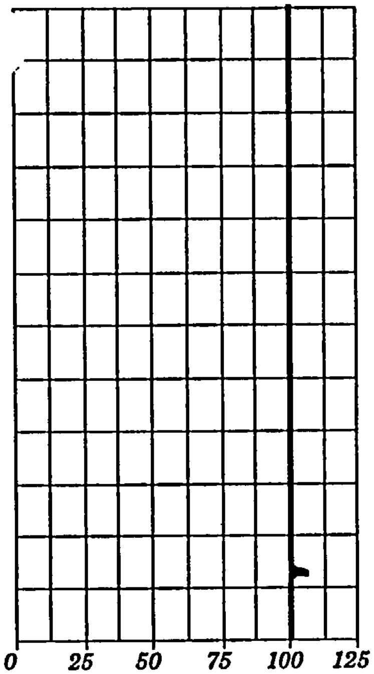


Transient # 11

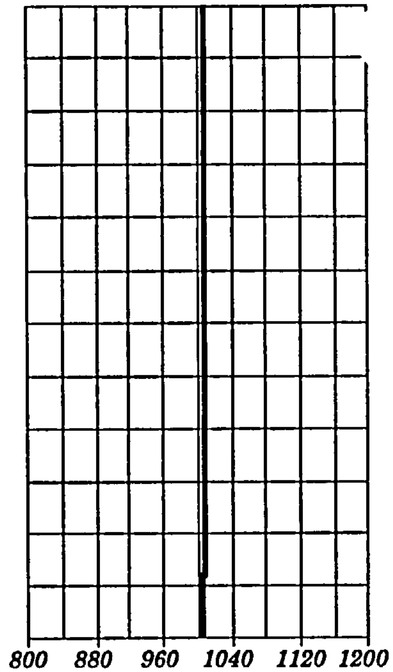


Transient #12
February 16, 1995
Rev. 1

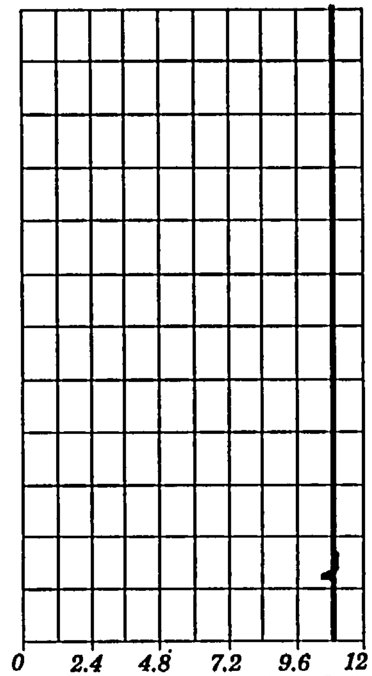
Transient #13



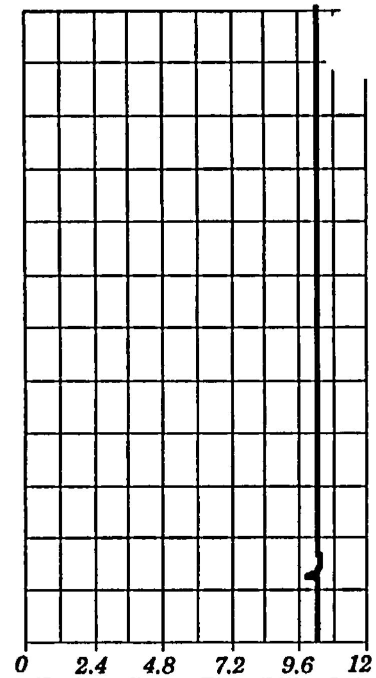
APRM "A" (%)



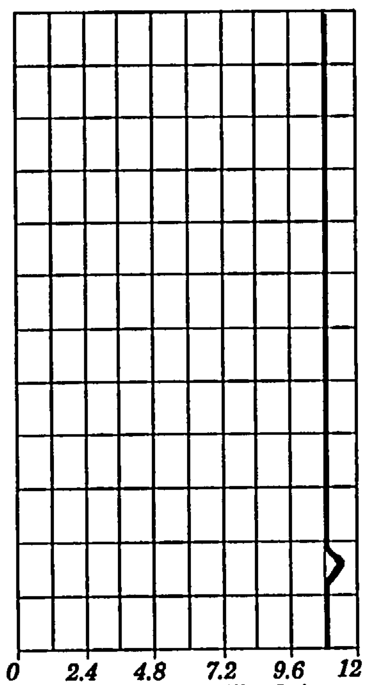
Rx. Pressure (PSIG)



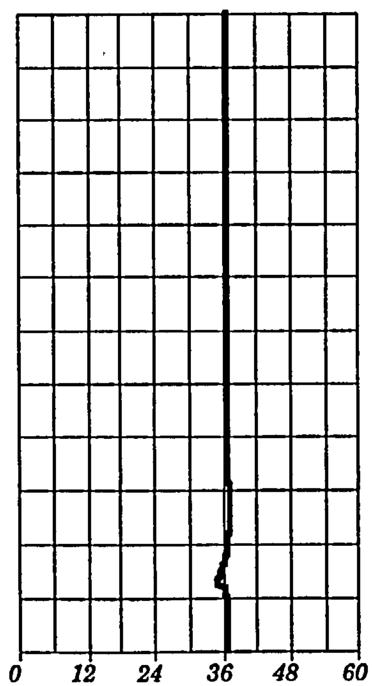
Reactor Steam Flow (Mlbm/hr)



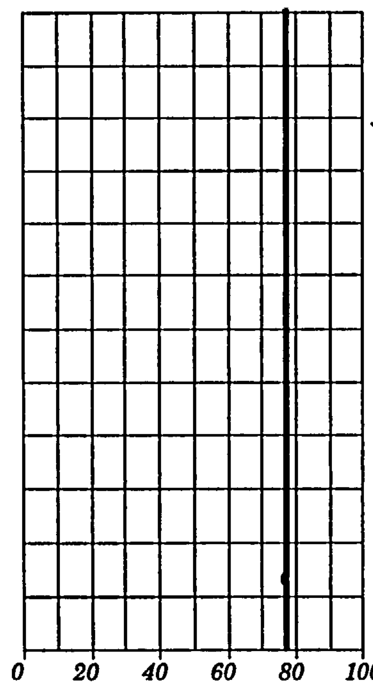
Turbine Steam Flow (Mlbm/hr)



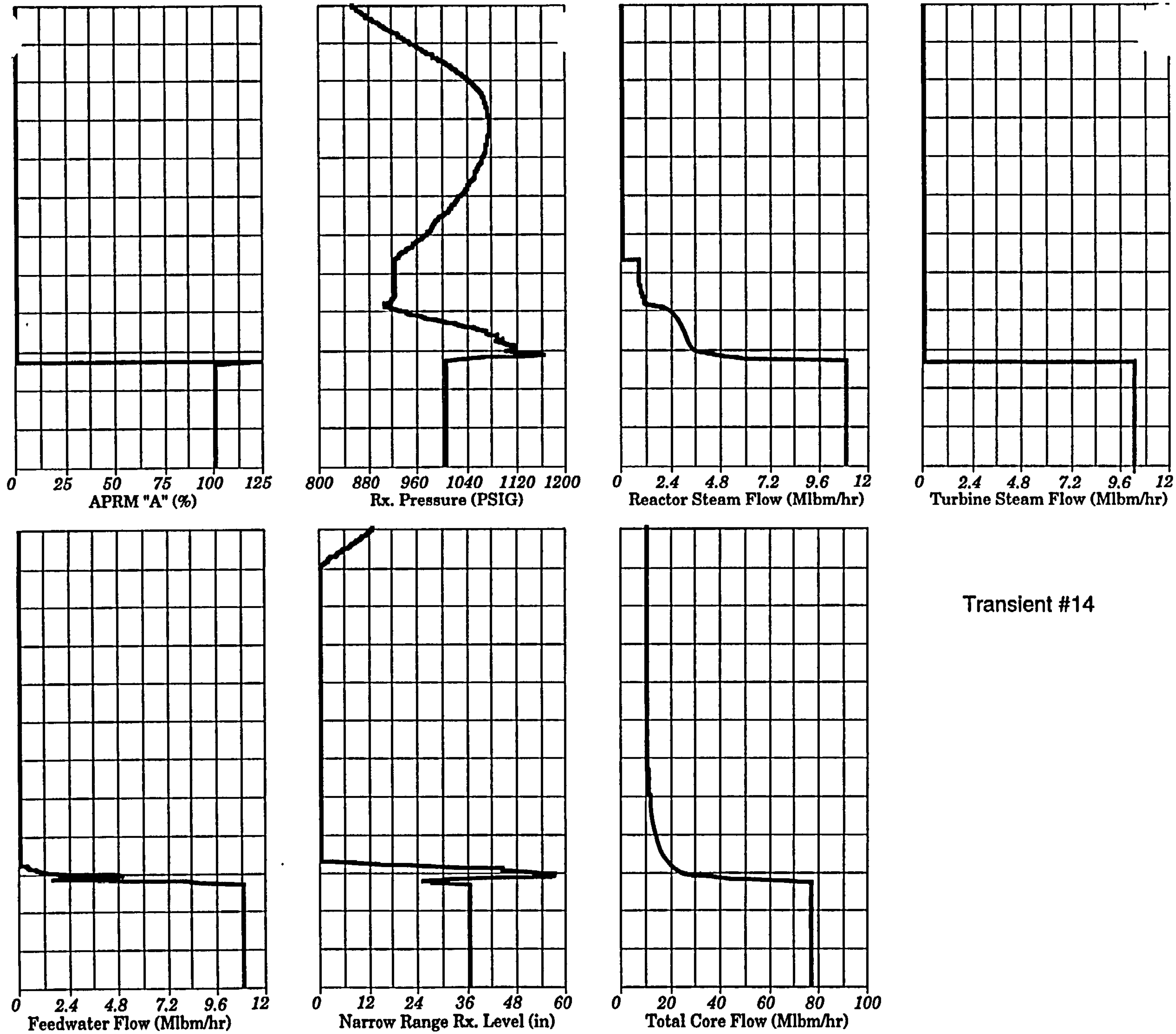
Feedwater Flow (Mlbm/hr)



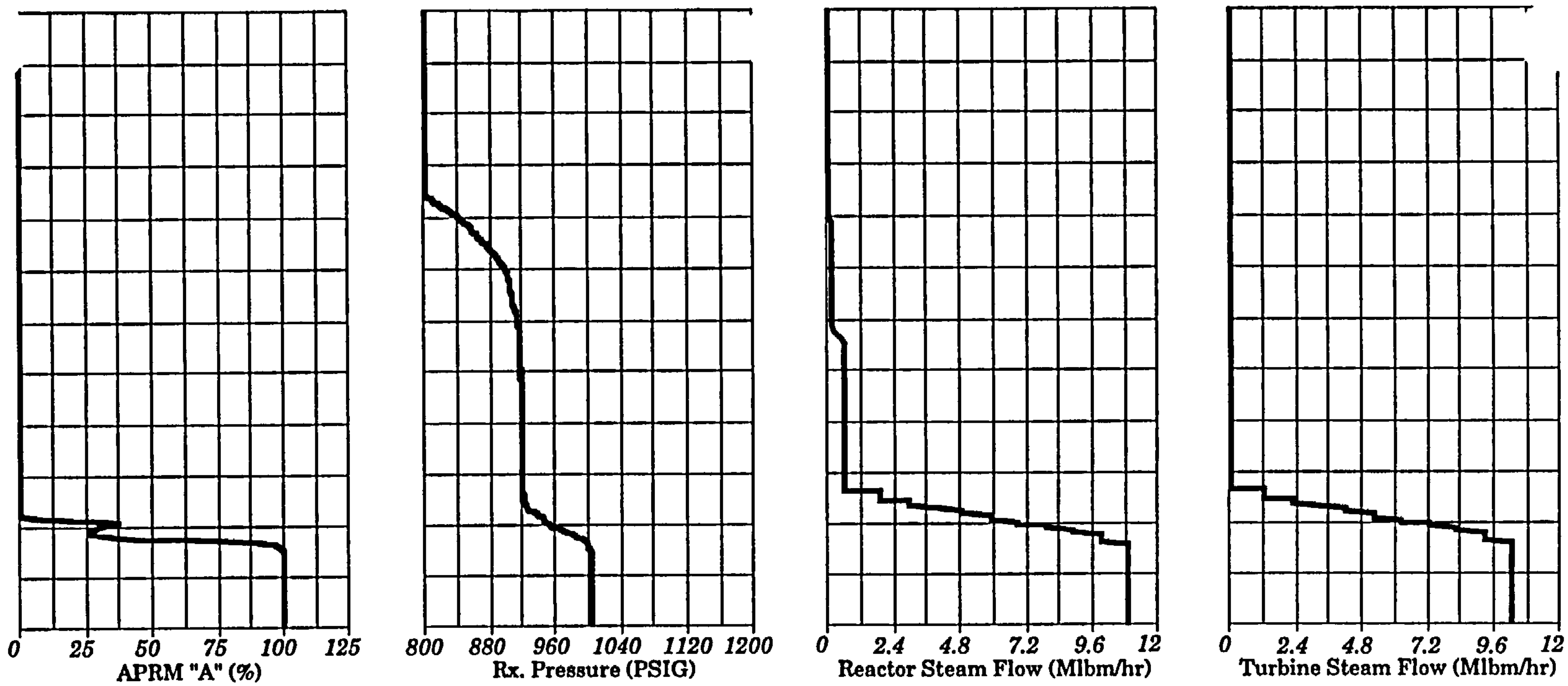
Narrow Range Rx. Level (in)

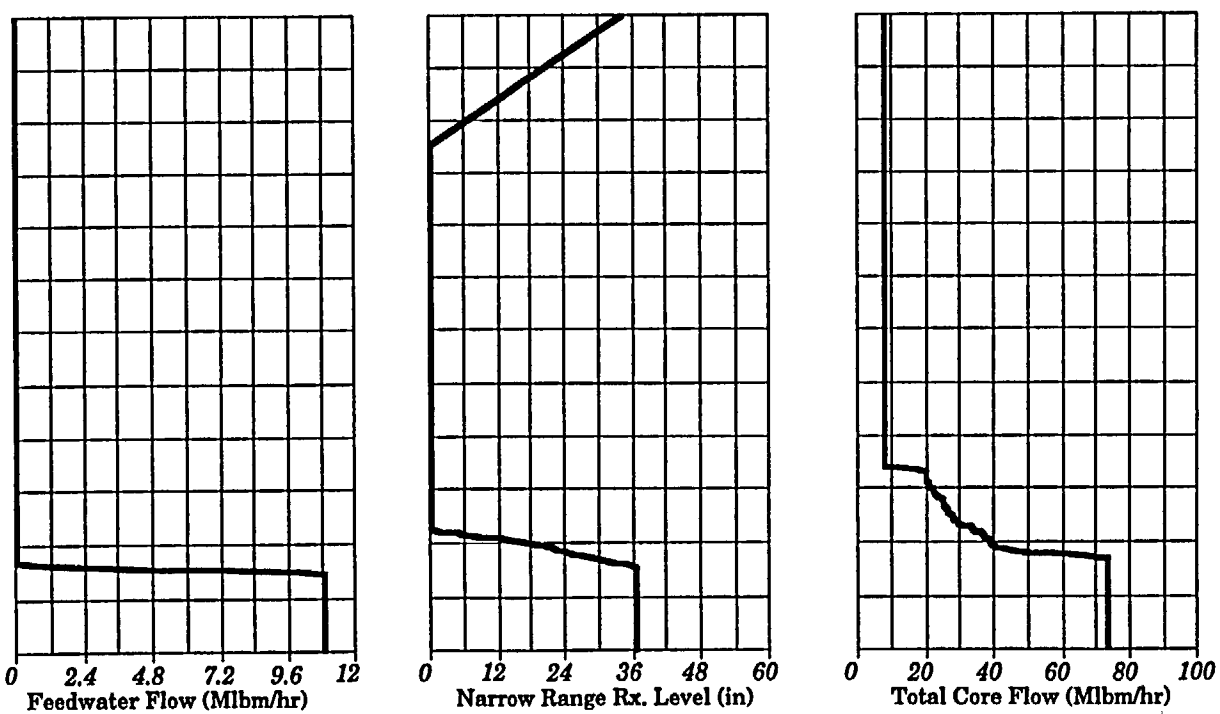


Total Core Flow (Mlbm/hr)

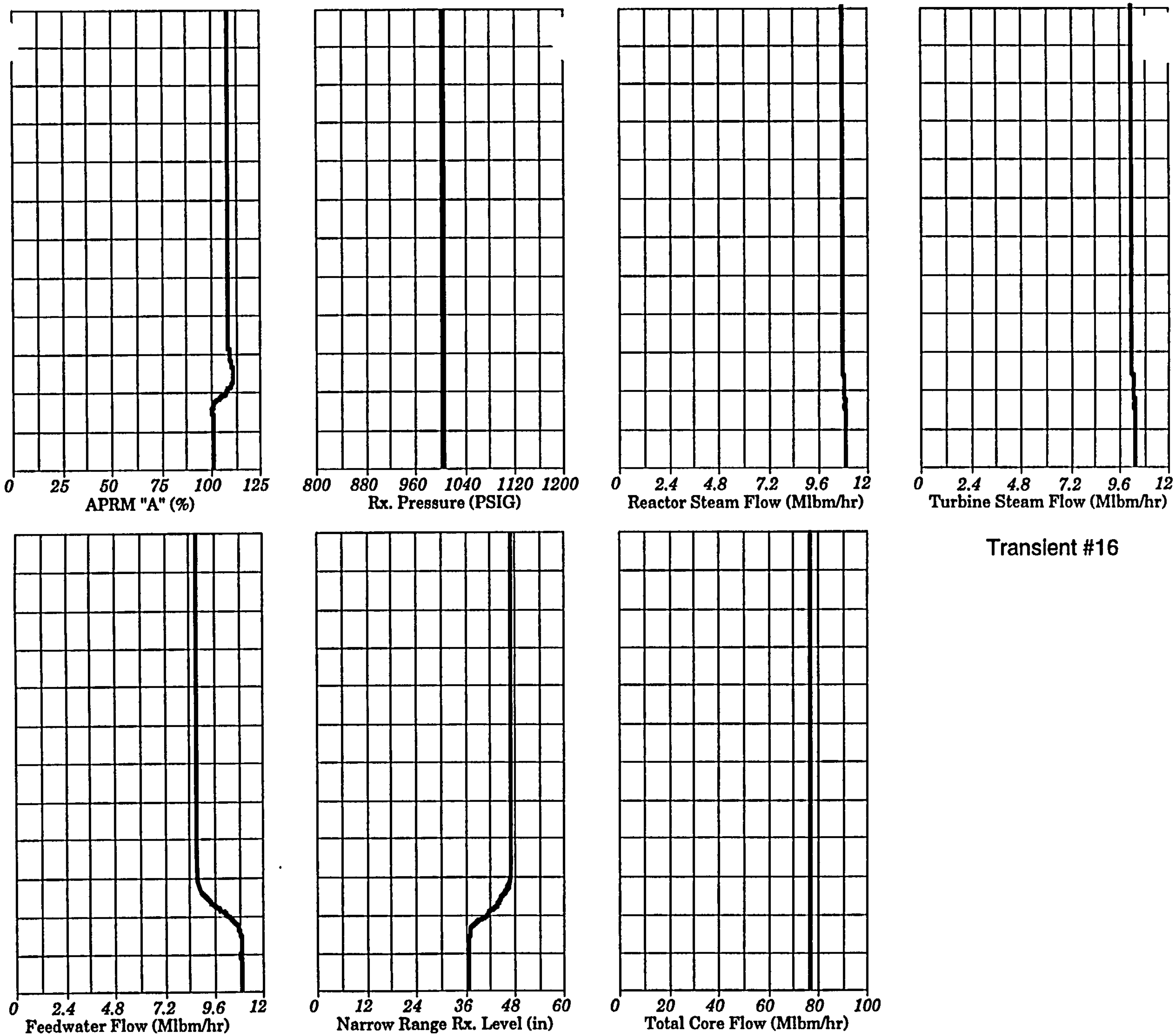


Transient #14

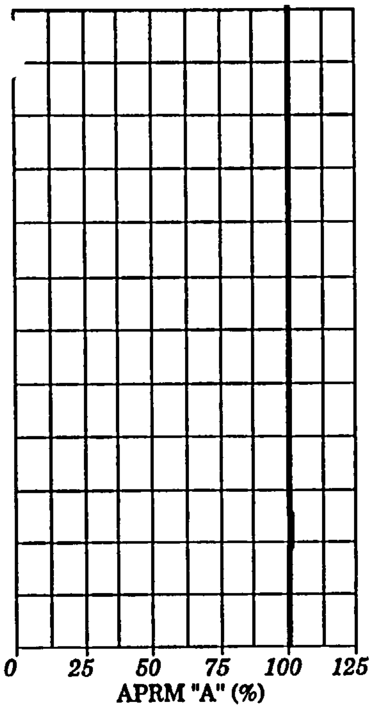


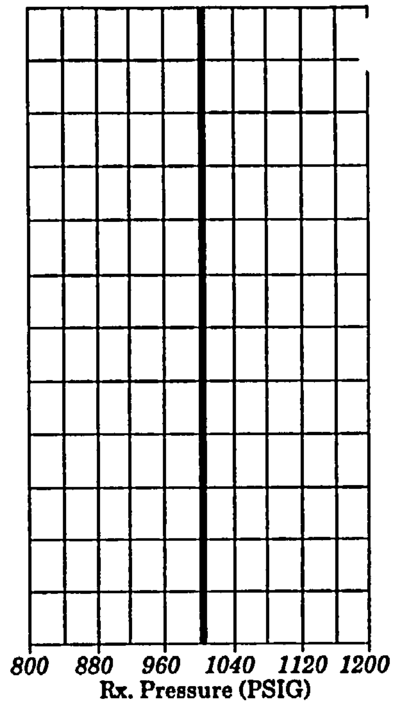


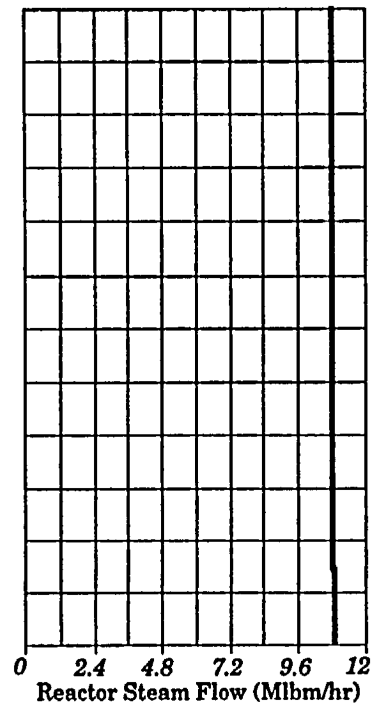
Transient #15
February 16, 1995
Rev. 1

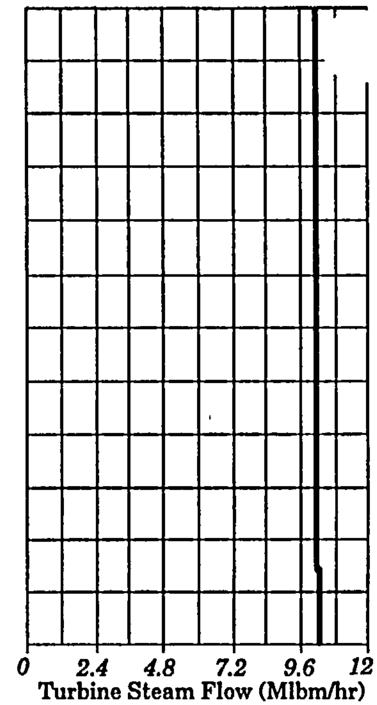


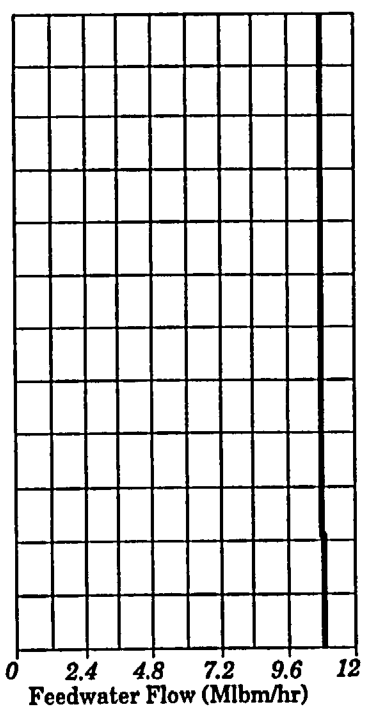
Transient #16

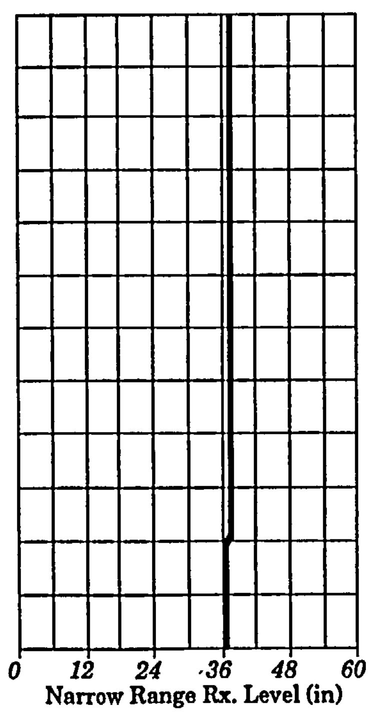


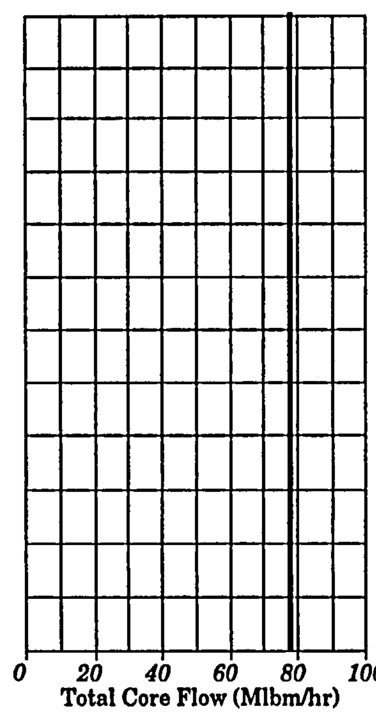




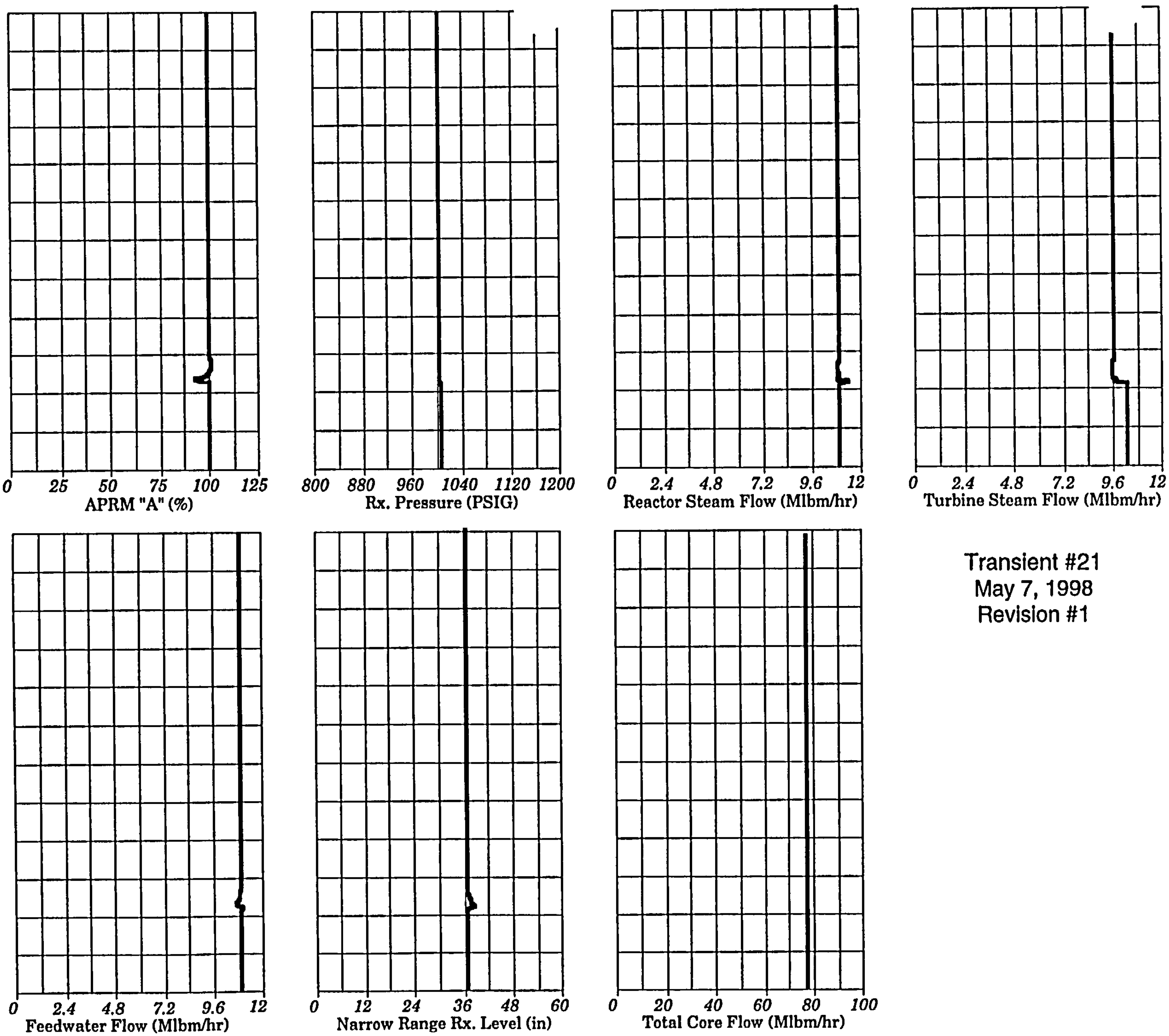




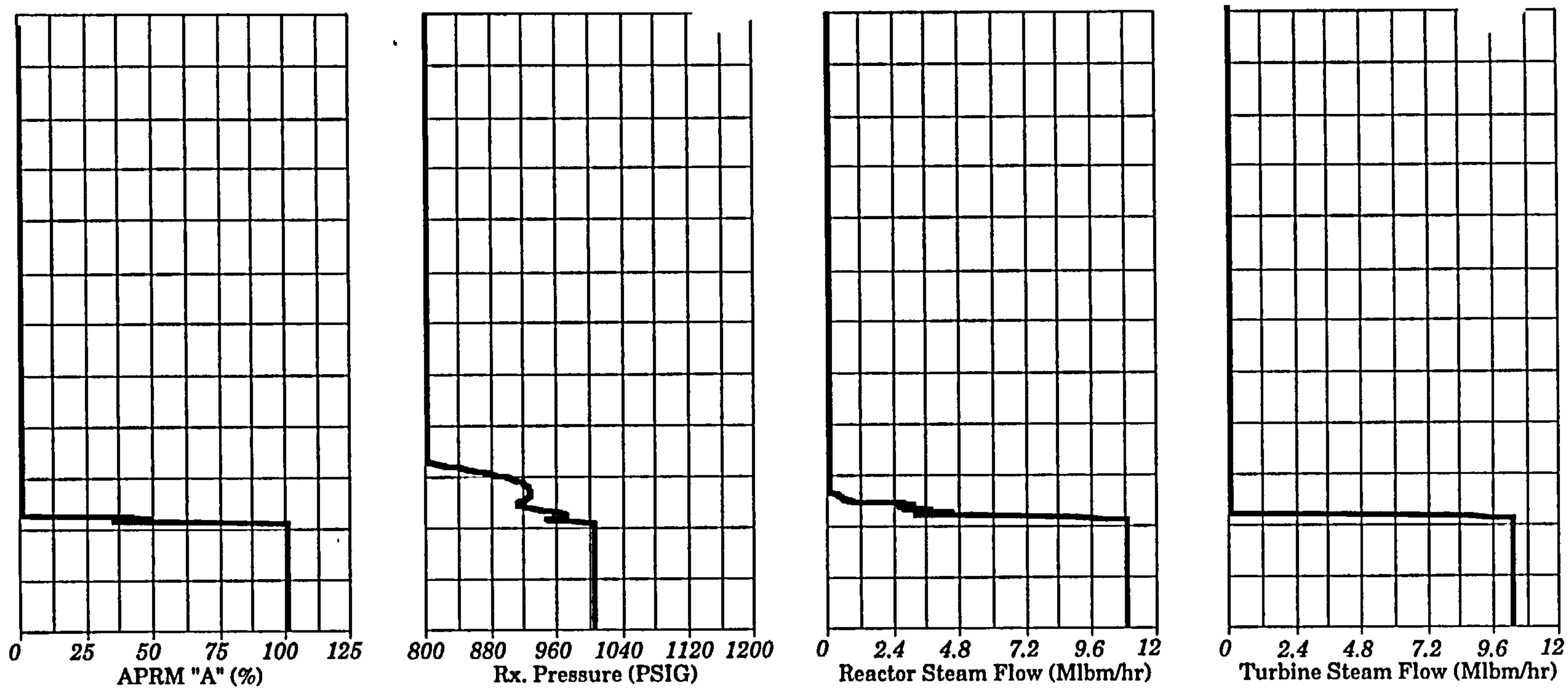


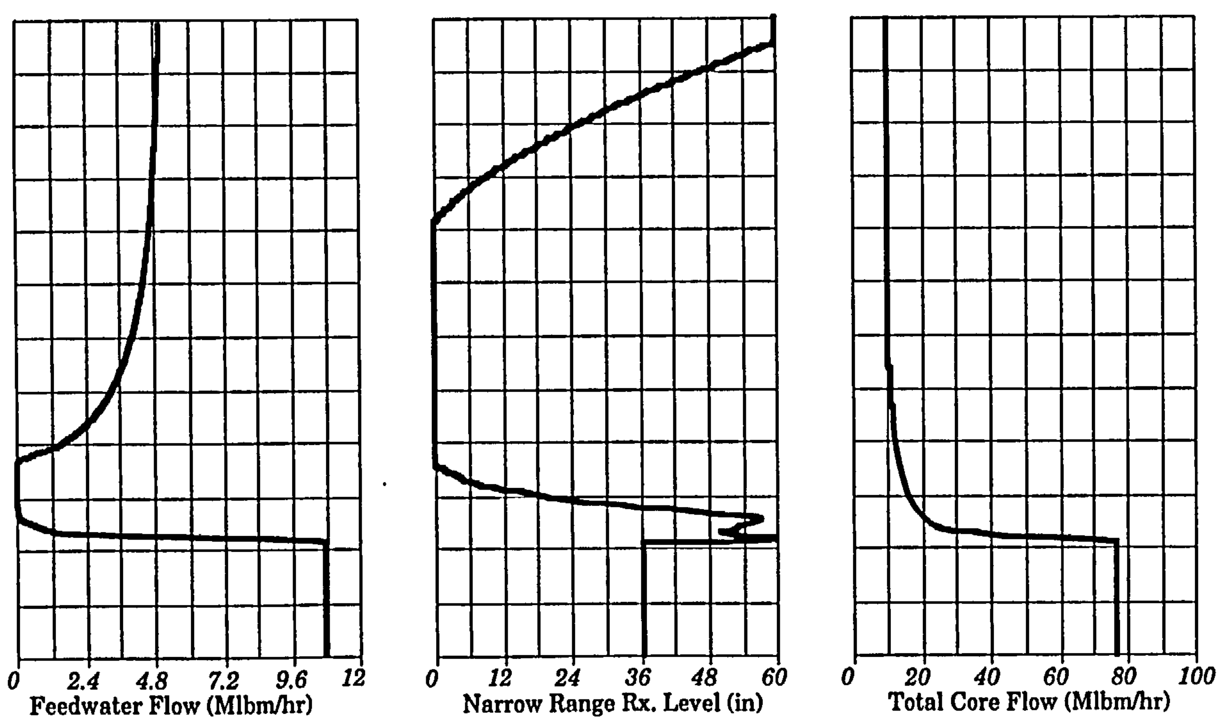


Transient #18
February 15, 1995
Rev. 1



Transient #21
May 7, 1998
Revision #1





Transient #22
May 4, 1998
Revision 1